Universidad Zaragoza
1542

Trabajo Fin de Grado

Virtualización y securización de nodo SIMACET para su uso en unidades de entidad Pequeña Unidad

Autor

Rodrigo Abenia Gracia

Director/es

Director académico: Ph. D. Dña. Lacramioara Dranca
Director militar: Capitán D. Manuel Landáburu de Lossada

Centro Universitario de la Defensa-Academia General Militar
2018

Agradecimientos

Mediante estas palabras, quiero agradecer, en primer lugar, a los profesores de la Academia General Militar y del Centro Universitario de la Defensa, la formación que he recibido durante estos últimos seis años.

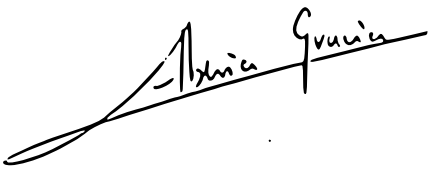
En segundo lugar, agradecer a la profesora Dña. Lacramioara Dranca, que desde el primer momento, y con su tediosa labor como tutora académica, ha permitido e impulsado la finalización de esta memoria, sin la cual, hubiera resultado muy difícil de conseguir.

Por otro lado, me gustaría agradecer al Capitán D. Manuel Landáburu de Lossada su inestimable aportación no solo en la consecución de este trabajo, sino también en la acogida que me brindó, haciendo de mi estancia en Ceuta un grato recuerdo para el futuro, y en las lecciones diarias de cómo lograr ser un buen Oficial.

Además, me gustaría agradecer a todo el personal de la Compañía de Transmisiones 17 de Ceuta el cariñoso trato que me brindaron, sintiéndome desde el primer día un integrante más de la Compañía, dejándome con ganas de volver a esta Unidad.

Por último, y no menos importante, agradecer a mi familia el apoyo recibido durante estos últimos años, sin los que hubiera sido difícil afrontar ciertas situaciones.

En Hoyo de Manzanares, a 14 de marzo de 2018



CAC. TRA. D. Rodrigo Abenia Gracia

Resumen

En cualquier empresa, la información es un activo esencial en el funcionamiento de esta, mas aún si se habla del Ejército de Tierra. En el ámbito militar, esta cobra un valor muy importante, jugando, en ocasiones, un papel fundamental en la conducción de operaciones armadas. Para apoyar al Mando en esta conducción, el Ejército posee el Sistema de Información para el Mando y Control en el Ejército de Tierra (SIMACET), el cual provee de los servicios necesarios al Jefe y a sus auxiliares en la toma de decisiones.

Los crecientes avances tecnológicos, unido a la necesidad de utilizar Sistemas de Información como SIMACET, han hecho que desde las Compañías de Transmisiones se comience a pensar en utilizar la virtualización en los Sistemas de Información militares. Este Trabajo Fin de Grado constituye un primer paso en la aplicación de dicha tecnología.

Para ello, se establece como objetivo crear un nodo SIMACET virtualizado y correctamente securizado que dé servicio a Pequeñas Unidades. Estableciendo como tareas intermedias: la creación de un manual inicial para establecer y configurar las máquinas virtuales necesarias, el desarrollo de un análisis de riesgos del Sistema virtualizado y un análisis de las ventajas y desventajas obtenidas de la aplicación de la virtualización.

Se concluye que la aplicación de la virtualización con hipervisor de tipo 2 es una opción más que factible, permitiendo desplegar los servicios de SIMACET de una forma más eficiente, utilizando los medios materiales y humanos de los que ya disponen las Compañías de Transmisiones.

Abstract

In any enterprise, information plays an important role on it, even more if it is the Army. In military field, information has a great value, being sometimes an important part in the management of armed operations. In order to support the Commander, the Army has the Information System for Command and Control in the Army (ISCCA), which provides the necessary services for the Commander and their assistants.

The increased technological advances, linked to the necessity to use Information Systems like ISCCA, have caused that many Signal Companies considerate to use the virtualization in military Information Systems. This Final Degree Project is a first step in the application of the virtualization technology.

To do this, it is established the objective of creating a ISCCA virtualized node and a properly hardening for Little Units. Some intermediate tasks are established: creation of an initial guide to create and configure necessary virtual machines, the development of a risks analysis and an advantages and disadvantages analysis of using virtualization.

The conclusions show that using a type 2 hypervisor is a really viable option, which allows to deploy ISCCA in an efficient way, using the material and human resources which already exist in the Army.

Lista de acrónimos

ACING	Academia de Ingenieros
AD DS	Active Directory Domain Server
BDT	Base de Datos Táctica
BZ	Batallón de Zapadores
CCN	Centro Criptológico Nacional
CG	Cuartel General
CGTAD	Cuartel General Terrestre de Alta Disponibilidad
CIS	*Communication and Information Systems* *Sistemas de Comunicación e Información*
CISCC	*CIS Control Center* Centro de Control de los medios CIS
CPU	*Central Processing Unit* Unidad Central de Procesamiento
GACA	Grupo de Artillería de Campaña
GL	Grupo Logístico
GPO	Group Policy Object Directiva de Grupo
GT	Grupo Táctico
GU	Gran Unidad
HW	Hardware
IP	*Internet Protocol* Protocolo de Internet
LAN	*Local Area Network* Red de Área Local
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
OTAN	Organización del Tratado del Atlántico Norte
PC	Personal Computer
PCALT	Puesto de Mando Alternativo

PCAV	Puesto de Mando Avanzado
PCR	Puesto de Mando Retrasado
PEXT	Prácticas Externas
PLMM	Plana Mayor de Mando
PU	Pequeña Unidad
RAM	*Random Access Memory* Memoria de Acceso Aleatorio
RRC	Red Radio de Combate
SIMACET	Sistema de Información para el Mando y Control del Ejército de Tierra
SINFO	Sistemas de Información
SO	Sistema Operativo
STIC	Servicio de las Tecnologías de la Información y las Comunicaciones
SW	Software
TFG	Trabajo de Fin de Grado
TICs	Tecnologías de la Información y la Comunicación
UO	Unidades Organizativas
VM	*Virtual Machine* Máquina Virtual
VMM	*Virtual Machine Monitor* Monitor de máquina virtual

Índice de contenidos

Índice de tablas

Índice de figuras

1. Introducción

El presente Trabajo de Fin de Grado (TFG) ha sido realizado durante el desarrollo de las Prácticas Externas (PEXT) en la Compañía de Transmisiones 17 de la Comandancia General de Ceuta en el Acuartelamiento “El Jaral” en Ceuta.

En los últimos años, la virtualización de servidores ha abierto un amplio abanico de posibilidades en los Sistemas de Información, permitiendo reducir el número de estos y, por ello, los costes ocasionados por tales, ya sean de mantenimiento o de energía consumida, siendo aplicada tanto en el ámbito civil como en el militar. Además, dicha tecnología ha permitido también, una creación y gestión de las redes de información más eficiente y rápida.

Teniendo en cuenta lo anterior, y observando las redes desplegadas y los cometidos de una Compañía de Transmisiones del Ejército de Tierra, la unidad en la que se han realizado las Prácticas Externas plantea aplicar la virtualización al Sistema de Información para el Mando y Control del Ejército de Tierra (SIMACET) para su explotación en unidades de entidad Pequeña Unidad (PU)[1].

Por otro lado, el despliegue de una red de SIMACET no sólo implica el establecimiento y configuración de las comunicaciones, sino que también establecer la seguridad necesaria que asegure el correcto funcionamiento de la red desplegada así como la confidencialidad de la información. La importancia de la seguridad es vital, puesto que la información que una unidad militar genera y recibe es material sensible que muy frecuentemente está clasificando, siendo en muchas ocasiones documentos o posicionamiento de unidades.

1.1 Objetivos y alcance

La problemática principal es la inexistencia de una guía o manual oficial para uso interno de las Fuerzas Armadas y la carencia de formación del personal militar en materia de virtualización. Por ello, la unidad propone el desarrollo de un manual, el cual se conforma con este trabajo, que sirva como guía para la creación de un nodo virtualizado de SIMACET para unidades de entidad PU, la cual tiene la incorporación de la virtualización como característica principal.

El objetivo de este trabajo es crear un nodo SIMACET virtualizado y correctamente securizado que dé servicio a Pequeñas Unidades. Para ello se pretende:

- Desarrollar un manual para la correcta instalación y configuración del software necesario para establecer un nodo virtualizado a nivel de PU.
- Realizar un análisis de riesgos.
- Realizar un análisis de ventajas y desventajas de usar la virtualización en este caso.

Para realizar el manual se va a partir de la experiencia propia instalando y configurando el software necesario, teniendo en cuenta las indicaciones del personal de la Compañía de Transmisiones 17 y de la Academia de Ingenieros.

Para un adecuado análisis de riesgos, y basándose en una aplicación oficial del Estado español, se va a hacer uso de la metodología MAGERIT, elaborada por el Consejo Superior de Administración Electrónica. Esta aplicación consta de tres versiones, siendo la última de ellas, la versión 3, la que se va a utilizar en la presente memoria.

---

[1] El termino Pequeña Unidad hace referencia a unidades de entidad Regimiento e inferior.

El caso que se va a tratar en esta memoria es un caso aislado de establecimiento de un nodo SIMACET, es decir, cabe la posibilidad de que cualquiera de las Compañías de Transmisiones del Ejército de Tierra haya desarrollado un nodo virtualizado de una forma diferente a la planteada en el presente trabajo. Además se ha de tener en cuenta que la propuesta de virtualización del Sistema mencionado es un caso simplificado del mismo, provocando que en muchas ocasiones las conclusiones obtenidas se basen en una visión general del mismo.

Se considera necesario concretar también la idea de que este trabajo sirva como base en la aplicación de la virtualización a los Sistemas de Información militares, no solo en SIMACET, tratando de explotar al máximo los medios humanos y materiales de los que ya dispone el Ejército de Tierra.

1.2 Ámbito de aplicación

Se ha de tener en cuenta, que aunque el trabajo ha sido a propuesta de la Compañía de Transmisiones 17 de Ceuta, los resultados obtenidos en este pueden ser de aplicación para cualquier Compañía de Transmisiones del Ejército de Tierra, dado que todas disponen de los medios humanos y materiales necesarios para el despliegue del conjunto de servicios que forman SIMACET, estando agrupados orgánicamente en la Sección SINFO[2] de una Compañía de Transmisiones.

Por otro lado, cabe destacar la posibilidad de utilización de la tecnología de virtualización para cualquier otro servicio que el Ejército de Tierra despliegue. Teniendo en cuenta lo anterior, los servidores de las redes desplegadas en los Puestos de Mando[3] de cualquier entidad, tanto PU como GU[4], podrían ser virtualizados.

1.3 Antecedentes

Pese a que la tecnología de virtualización se utiliza en el ámbito civil desde principios de siglo, en el ámbito de Defensa no ha sido hasta los últimos 2 ó 3 años (1) cuando se ha comenzado a pensar en la posibilidad de virtualizar los sistemas militares.

La primera unidad que consiguió virtualizar SIMACET fue el Regimiento de Transmisiones 21, situado en Marines (Valencia). Dada su proximidad al Cuartel General Terrestre de Alta Disponibilidad (CGTAD) de la OTAN, situado en Bétera, es necesario que los medios y tecnologías utilizados estén acordes a los actuales en telecomunicaciones civiles. Por ello, el Regimiento utilizó la virtualización, utilizando software de VMware de hipervisor tipo 1, en el montaje de Puestos de Mando para su uso en unidades de entidad Gran Unidad, disponiendo de un importante despliegue de medios, tanto económicos como de personal, montando estos para un gran número de usuarios.

A diferencia de lo realizado en Valencia, este trabajo está enfocado a la utilización de la tecnología de virtualización a nivel PU, implicando unos medios materiales y humanos menores a los del Regimiento de Transmisiones mencionado.

---

[2] El término Sección SINFO hace referencia a la Sección que la doctrina del Ejercito establece para encargarse de los Sistemas de Información (ej.: SIMACET).

[3] Un puesto de Mando es el lugar donde se concentran todos los Sistemas de Mando y Control, así como las transmisiones necesarias para apoyar al Mando en la toma de decisiones.

[4] El termino Gran Unidad hace referencia a unidades de entidad Brigada o superior.

Por otro lado, personal de la Especialidad Fundamental de Transmisiones, y de forma no oficial, han tratado de implementar la virtualización en numerosos sistemas y/o servicios militares no llegando a materializarse en un manual o documento militar oficial.

1.4 Estructura de la memoria

La estructura que se va a seguir consta de cuatro partes diferenciadas: análisis de SIMACET y explicación del mismo; aplicación de la tecnología de virtualización al Sistema de Información; instalaciones y configuraciones iniciales para el establecimiento de los servicios necesarios; y análisis de riesgos del Sistema en su conjunto.

La primera de las tres partes se basa en la publicación doctrinal militar PD3-602 "Establecimiento y empleo de SIMACET", la cual establece, por un lado la estructura del Sistema, en términos tanto de servicios como de usuarios, y por otro, el establecimiento del mismo para su explotación por parte de los usuarios.

En cuanto a virtualización, en primer lugar se explica la elección del tipo de hipervisor y modelo a utilizar, detallando la forma en que se va a aplicar dicha tecnología, para a continuación aplicarla al Sistema en cuestión.

Mediante manuales realizados personalmente, se explican las instrucciones iniciales necesarias para el establecimiento de las máquinas virtuales necesarias en el despliegue de un Puesto de Mando. Los manuales mencionados se encuentran en su totalidad en los Anexos E, F y G, aunque en el apartado 4 se mencionan y explican los puntos más importantes.

A continuación, se realiza un análisis de riesgos aplicando la metodología MAGERIT v3 a través de la aplicación PILAR, llegando a las conclusiones finales para el establecimiento de SIMACET.

2. Análisis del sistema

2.1 Concepto

Mediante la función de combate mando y control (2), el Mando militar ejerce la autoridad sobre sus unidades subordinadas, con el fin de dirigirlas en el cumplimiento de la misión asignada. Para ello, el jefe militar dispone de una serie de Sistemas de Información y Comunicación que le apoyan en la toma de decisiones. Uno de estos es el Sistema para el Mando y Control del Ejército de Tierra, al cual se debe el presente trabajo.

Dicho sistema ofrece al usuario aplicaciones de diferentes tipos, donde se pueden destacar las siguientes:

- Aplicaciones de gestión táctica.
- Aplicaciones de información geográfica.
- Aplicaciones de mensajería**.**

El núcleo principal del sistema (3) es la base de datos táctica (BDT). Esta puede definirse como el conjunto de datos base de iconografía, plantillas, grupos y perfiles de usuario y de datos planeados de usuarios, de red del sistema y de información táctica. Los datos mencionados son cargados en los nodos que van a intervenir en la maniobra, consiguiendo con esto que todos dispongan de la misma información inicial.

Una vez la maniobra ha dado inicio, los cambios que se produzcan en la BDT son actualizados en todos los nodos del sistema. Para que dichos cambios sean transferidos a todos los usuarios se utiliza un mecanismo de réplica[5].

2.2 Composición del Sistema

La composición de SIMACET se basa en tres elementos:

- Nodos: se asocian unos con otros, creando las redes lógicas de réplica, las cuales permiten la actualización de los datos de la BDT.
- Redes lógicas de réplica: a través de las cuales se difunden y filtran los datos de la BDT.
- Usuarios: responsables de introducir y gestionar la información dentro del sistema.

2.2.1 Nodos

Un nodo está definido como el conjunto de medios, HW y SW, capacidades, personal y procedimientos que realizan todas o algunas de las funciones del sistema. Cada nodo dispone de la BDT que intercambia información con la de otros nodos. El conjunto de varios nodos junto con los procedimientos adecuados conforman la red de SIMACET.

Además, se pueden diferenciar varios tipos de nodos:

- Nodos fijos: son los creados para ser instalados en una posición fija, los cuales están enfocados a ser utilizados en Centros de Enseñanza Militar o en la Red Estratégica Militar[6].
- Nodos desplegables: son los creados para ser proyectados a cualquier territorio y ser empleados por los usuarios que conforman un Puesto de Mando. Es el tipo de nodo que una Compañía de Transmisiones despliega.
- Nodo aislado: es el creado para ser utilizado por un usuario o por un elemento de control de red (CISCC).
- Nodos pasarela: son los creados para filtrar la información táctica y puede ser asociado a dos o más redes lógicas. Se debe tener en cuenta que cualquier nodo puede ser empleado como nodo pasarela.

2.2.2 Redes lógicas de réplica

Con el fin de difundir y actualizar la información táctica, agrupada en la BDT, los nodos se agrupan en redes lógicas de réplica, consiguiendo de esta manera, que los nodos integrados en esta red posean idéntica información.

---

[5] Réplica en bases de datos se entiende como la técnica mediante la cual la base de datos es copiada íntegramente en otra ubicación. Con esto se permite que la base de datos puede ser utilizada y actualizada en varias ubicaciones diferentes al mismo tiempo.

[6] Red permanente en territorio nacional.

Para interconectar diferentes redes lógicas de réplica se utilizan los nodos pasarela, consiguiendo además la aplicación de filtros para la información táctica que discurra entre redes distintas.

Además, existen tres tipos de redes lógicas[7] diferentes, atendiendo al procedimiento utilizado para la transmisión de la información táctica:

- Red de réplica tipo IP de SIMACET.
- Red de réplica tipo LAN de SIMACET.
- Red de réplica tipo RRC de SIMACET.

2.2.3 Usuarios

Dentro de SIMACET existen dos tipos de usuarios bien definidos y diferenciados:

- Usuarios técnicos: son los encargados de la administración de los nodos del sistema.
- Usuarios de CG/PLMM: son los usuarios que explotan el sistema. Están asignados a un nodo en concreto, aunque si la situación lo requiriera podrían acceder al Sistema desde otros nodos.

Para el establecimiento de los usuarios se crean una serie de perfiles, los cuales se asignan a cada grupo de usuarios. Dichos perfiles permiten dar acceso o denegarlo a ciertos recursos y/o servicios disponibles en el sistema.

3. Selección de solución de virtualización a emplear

3.1 Concepto de virtualización

En primer lugar, es preciso entender el concepto de virtualización (4), el cual se define como el proceso de creación de una representación virtual de un elemento, a través de un SW, en lugar de una representación física del mismo. A efectos prácticos y a nivel usuario, virtualizar es crear uno o varios elementos software (por ejemplo, sistemas operativos) en un equipo donde "tradicionalmente" solo se podría ejecutar un solo elemento software. Los sistemas informáticos virtuales que se crean son conocidos como "máquinas virtuales". Para ello, se utiliza un software de virtualización alojado en un host físico denominado host anfitrión, el cual crea una capa de abstracción entre el hardware de la maquina física (host anfitrión) y la máquina virtual, la cual es gestionada mediante el hipervisor.

Para entender mejor la tecnología de virtualización se debe comprender qué es el hipervisor. El hipervisor o Monitor de Máquina Virtual (VMM) es aquella plataforma encargada de la creación y gestión de la capa de abstracción que permite la creación de las máquinas virtuales, es decir, la capa intermedia entre el hardware y las máquinas virtuales, como se puede apreciar en las figuras 3.1 y 3.2 y en sus respectivas explicaciones. Como consecuencia, utiliza y gestiona los cuatro recursos principales de una máquina virtual: CPU, memoria, red y almacenamiento. En el siguiente apartado se van a explicar los diferentes tipos de hipervisor existentes y el elegido para el presente trabajo.

---

[7] Se encuentran detalladas en el Anexo A

Cabe destacar que la capa mencionada es la que permite la creación y gestión de varios host virtuales dentro de un único host físico, haciendo posible un uso más eficiente de los recursos, lo que la convierte en la parte fundamental de la virtualización.

Cada máquina virtual (VM) cuenta con su propio sistema operativo (Linux, Windows,…) siendo el host anfitrión físico el que asigna una parte de sus recursos totales, gestionados por el hipervisor del software de virtualización.

3.2 Tipos de hipervisor

En el mercado actual existen dos tipos de hipervisores:

1. Hipervisor tipo 1: denominado también nativo, unhosted o bare-metal, es el hipervisor que se ejecuta directamente sobre el hardware físico, antes que ningún otro de los sistemas operativos virtualizados, tal y como puede observarse en la figura 3.1, donde el hardware real o físico se encuentra justo por debajo del hipervisor.

Para la gestión de las máquinas virtuales, el hipervisor ejecuta una interfaz que permite visualizar y gestionar las VMs que se hayan creado.

Este tipo de hipervisor es el primero que se creó siendo actualmente el utilizado en las máquinas virtuales más potentes.

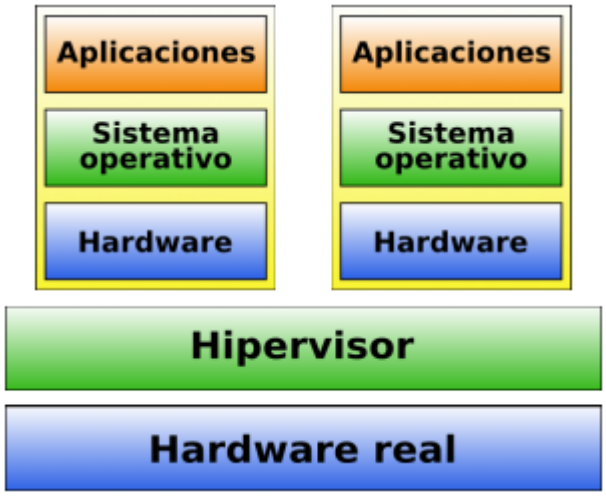


Figura 3.1 Hipervisor tipo 1
Fuente: Wikipedia

2. Hipervisor tipo 2: denominado también hosted, es el hipervisor que se ejecuta sobre un sistema operativo completo instalado previamente, es decir, entre el hipervisor, o software de virtualización en este caso, se encuentra el Sistema Operativo del host físico que actúa como anfitrión, mostrado en la figura 3.2.

Este tipo de host es el más utilizado a nivel usuario, ya que, puede ser utilizado en cualquiera de los sistemas operativos creados para ser empleados por un usuario independiente.

Figura 3.2 Hipervisor tipo 2
Fuente: Wikipedia

En el presente trabajo se va a hacer uso de un hipervisor tipo 2, puesto que este se instala sobre un sistema operativo, lo que hace que esta opción sea la más accesible, para cualquier Compañía de Transmisiones que desee virtualizar SIMACET, por varios motivos:

1. Es la opción más económica, puesto que el software de virtualización utilizado es el mismo que se utiliza a nivel usuario, lo que implica que el coste de las licencias es mucho menor.

2. No es necesario disponer de un servidor físico para su uso, sino que con un ordenador personal se puede virtualizar directamente. A diferencia de SIMACET de GU, que precisa de unos mayores recursos, SIMACET de PU, precisa de un menor número de estos, pudiendo ser cubiertos por un ordenador personal con unas características determinadas.

En relación al motivo 1, los costes que la empresa desarrolladora de VMware Workstation ha establecido para cada tipo de producto son los siguientes[8]:

- Producto para hipervisor tipo 1: vSphere Essentials Kit. Tiene un coste anual de 639,94 euros.

- Producto para hipervisor tipo 1: vSphere Essential Plus Kit. Ofrece más capacidades que la versión Essentials Kit. Tiene un coste anual de 5160,54 euros.

- Producto para hipervisor tipo 2: VMware Workstation 14 Pro. Tiene un coste anual de 274,95 euros.

Como se puede observar, el software de hipervisor tipo 2, VMware Workstation 14 Pro, cuesta menos de la mitad que el utilizado en hipervisor tipo 1 en su versión Essentials Kit.

[8] Datos extraídos de la web oficial de VMware (www.vmware.com).

3.3 Modelos de virtualización

Dentro de la tecnología de virtualización existen también diferentes modelos de esta, donde se pueden destacar los siguientes:

1. Virtualización de plataforma.
2. Virtualización de recursos.
3. Virtualización de aplicaciones.
4. Virtualización de escritorio.

A continuación se van a explicar brevemente los diferentes modelos de virtualización para así poder entender mejor el alcance de dicha tecnología:

3.3.1 Virtualización de plataforma

Este es uno de los modelos más utilizados, siendo el principal a nivel usuario. Se entiende por virtualización de plataforma la creación de una maquinal virtual mediante la combinación de software (sistema operativo anfitrión y software de virtualización) y hardware (cada una de las partes físicas que componen el host anfitrión).

El host anfitrión es el encargado de crear un entorno virtual sobre el que se instalará la máquina virtual, que en este caso y en la mayoría de ocasiones será un sistema operativo completo, como por ejemplo, Windows 10.

Un ejemplo de este caso, y para que resulte más visual, es la figura 3.2, donde puede observarse por capas (hardware, sistema operativo y software de virtualización) la definición del párrafo anterior. Esta permite la creación de cuantas máquinas virtuales sean necesarias, pudiendo instalar en estas las aplicaciones o software que sea necesario.

3.3.2 Virtualización de recursos

Este modelo, y tal y como el nombre indica, se utiliza para la virtualización de recursos físicos, con el objeto de crear un recurso virtual y, de esta forma, gestionarlo de una manera más eficiente.

Este modelo de virtualización es comúnmente utilizado para la virtualización de recursos de almacenamiento.

3.3.3 Virtualización de aplicaciones

La virtualización de aplicaciones consiste en la ejecución de una aplicación determinada sin la necesidad de que esta haya sido instalada y configurada en el host anfitrión. Para ello, la aplicación mencionada está alojada en un paquete que contiene a esta y a todo el entorno necesario para la adecuada ejecución de la aplicación sin ser previamente instalada.

3.3.4 Virtualización de escritorio

Este modelo se basa en la separación entre el escritorio, utilizado por el usuario, y la máquina virtual. Esto implica que todos los programas, aplicaciones, procesos y datos que utiliza el usuario son almacenados en un servidor físico centralizado. Esto permite que el usuario pueda acceder de forma remota a dichos archivos desde cualquier host que pueda ejecutarlos remotamente.

3.4 Selección de modelo y software de virtualización

En el presente trabajo se va a hacer uso del modelo de virtualización de plataforma con hipervisor de tipo 2, siendo Windows 10 el sistema operativo del host anfitrión. Los argumentos que motivan dicha elección son los siguientes:

1. Cualquier Compañía de Transmisiones del Ejército de Tierra dispone de varios ordenadores personales para la ejecución de tantas máquinas virtuales como sean precisas, y de esta forma, poder realizar tantas pruebas y/o configuraciones distintas como sea necesario.
2. Es la opción que presenta un menor coste, puesto que el sistema operativo Windows 10 es el instalado actualmente en todos los equipos del Ejército de Tierra, no implicando ello un coste adicional.
3. Permite una formación del personal más sencilla, asequible y accesible. Sencilla porque se pueden crear, modificar y eliminar todas las máquina virtuales que sean necesarias, desde un solo equipo y sin afectar directamente a su hardware en caso de fallo; asequible, porque cualquier integrante del Ejército puede disponer de dicho SW en su casa y trabajar con las máquinas virtuales creadas para la formación.
4. La posibilidad de gestionar las máquinas virtuales que conforman SIMACET desde un ordenador personal. Esto es consecuencia del menor número de usuarios a los que se da servicio en un puesto de mando de PU.

Dentro de los diferentes software de virtualización de plataforma, con hipervisor tipo 2, existentes en el mercado destacan los siguientes:

- VMware Workstation de VMware Inc.
- VirtualBox de Oracle.
- Hyper-V de Microsoft.

Cabe destacar que el único gratuito es VirtualBox, pero se debe tener en cuenta que el soporte técnico[9] no es el más adecuado para un sistema a utilizar en una institución del Estado español. Teniendo en cuenta lo anterior, se decide utilizar el software VMware Workstation Pro versión 14 (5), siendo esta la opción que mejores servicios nos brinda, además de estar desarrollada por una empresa aprobada por el Ministerio de Defensa, con una variedad de productos, que en alguna otra ocasión ya han sido utilizados en el Ejército de Tierra, tal y como se ha mencionado en el apartado “Antecedentes”.

---

[9] Como puede observarse en la página web del producto (www.virtualbox.org), apartado Community, el soporte técnico se basa en la comunidad de usuarios.

Además, el producto VMware Workstation posee otra versión (VMware Workstation Player), la cual es similar a su versión Pro, pero con diferencias sustanciales que se exponen en "Anexo B: Comparativa entre versiones de VMware Workstation" en una tabla comparativa.

Al comparar dichas diferencias hacen que la decisión de utilizar la versión Pro sea evidente, dado que esta nos ofrece más servicios y capacidades (por ejemplo: ejecutar varias VMs al mismo tiempo o realizar instantáneas[10]), indispensables para la virtualización de un nodo SIMACET, que su versión más sencilla, la Player.

Por último, el software de virtualización tiene unos requisitos de software y hardware necesarios para su correcto funcionamiento, los cuales están detallados en el Anexo C. Se debe tener en cuenta que estos requisitos son los necesarios para el funcionamiento del software de virtualización en un ordenador personal, no un servidor, sirviendo como base para establecer los requisitos mínimos en la posible adquisición de uno.

De los requisitos detallados en el Anexo C se pueden extraer las siguientes conclusiones:

1. Aunque se recomienda que la memoria RAM sea de más de 4 GB, para el presente trabajo debe ser mayor, dependiendo del número de servicios que se van a dar y el número de usuarios que van a explotarlos.

2. Aunque no se especifica la capacidad de almacenamiento recomendada, en el caso de esta memoria, debe establecerse conforme a los servicios y usuarios, tal como se ha mencionado en el punto anterior.

3. Cualquier Windows Server, ya sea 2008 o 2012, son compatibles con VMware Workstation 14 Pro como host invitado en una máquina virtual, teniendo en cuenta que estos servidores son los utilizados en los sistemas del Ejército de Tierra.

4. Instalación de VMware y creación de las máquinas virtuales

Para la instalación y configuración del nodo SIMACET en su conjunto es necesaria la instalación de diferentes software, como son el software de virtualización y las máquinas virtuales a utilizar, las cuales van a ser explicadas a continuación. Para llevar a cabo dichas instalaciones me he basado en los conocimientos adquiridos durante el periodo de prácticas en Ceuta y a las asignaturas correspondientes estudiadas en la Academia de Ingenieros de Hoyo de Manzanares.

Se debe tener en cuenta que la memoria no va a contener todos los pasos necesarios para completar las diferentes instalaciones. Los manuales completos se encuentran en detalle en los anexos correspondientes, detallando en este apartado 4 los puntos más importantes a tener en cuenta en los procesos de instalación y configuración iniciales.

[10] Las instantáneas capturan el estado completo de la máquina virtual en el momento en que se crea la instantánea. Se pueden realizar en cualquier momento, ya sea, cuando se enciende la máquina virtual, cuando se apaga, o cuando se está ejecutando. Esta herramienta permite que en caso de fallo de la máquina, se puede volver a un estado anterior al fallo.

4.1 Instalación del software de virtualización

En primer lugar es necesaria la instalación del software de virtualización, que en este caso será VMware Workstation Pro versión 14, elegido como mejor opción en el apartado 3.4. Para ello y siguiendo los pasos establecidos según "Anexo E: Instalación de VMware Workstation 14 Pro" se va a proceder a explicar los puntos más importantes a tener en cuenta en dicha instalación:

1. La ubicación de los archivos será la que se establezca por defecto y los driver del teclado se instalarán, evitando así, posibles problemas en la interacción host físico-máquina virtual.

2. En el siguiente punto (paso 4 del Anexo E) se solicita permiso para comprobar posibles actualizaciones en el futuro, y el envío de informes a la empresa desarrolladora con el fin de mejorar el software. Este paso es importante como parte de la securización del nodo, puesto que si existiera una conexión a Internet en algún nodo, el hecho de comprobar posibles actualizaciones del SW, por un lado, y el enviar informes a los desarrolladores, por otro, podrían constituir una vulnerabilidad del sistema. Esta vulnerabilidad se produce al conectar el sistema a una red exterior, en este caso Internet, e intercambiar datos entre esta y la red creada para SIMACET. Este es el motivo por el cual todas las redes del Ejército están totalmente aisladas del exterior y trabajan de forma autónoma, siendo gestionadas por el personal de Transmisiones. Dado que el sistema no va a disponer de conexión a Internet, estas opciones no se marcan.

4.2 Creación de máquinas virtuales en VMware

En primer lugar es necesario explicar el concepto de servidor. Un servidor es un software capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia, es decir, un equipo que da uno o varios servicios a los clientes conectados a este. Un servidor puede tener muchos roles, donde se pueden destacar los de servidor de correo, servidor de archivos o servidor web.

Para el correcto funcionamiento del nodo virtual es necesaria la instalación de ciertas máquinas virtuales que funcionarán como servidores. Para el presente trabajo se tienen en cuenta cuatro VMs, necesarias para prestar los servicios mínimos que requiere un puesto de mando, que implementarán los siguientes servidores:

1. Controlador de dominio (Active Directory Domain Server).
2. Microsoft Exchange Server.
3. Microsoft SharePoint Server.
4. SIMACET (en Microsoft Windows Server).

Un controlador de dominio es el encargado de la autenticación y organización de los usuarios, es decir, del control de los usuarios que pueden hacer uso de los recursos "compartidos" en la red de SIMACET. Para ello, se va a hacer uso de la herramienta Active Directory Domain Server que Microsoft Windows Server incluye.

El servidor Microsoft Exchange es el encargado de establecer las herramientas necesarias que ofrecen un servicio de correo entre los usuarios que conforman SIMACET.

El servidor Microsoft SharePoint es utilizado para la creación de páginas web, espacios de trabajo compartidos y para almacenes de información y documentos.

El servidor SIMACET, alojado en un Windows Server, es el encargado de albergar el software propiamente dicho del Sistema militar, el cual posee las aplicaciones que posteriormente utilizarán los usuarios. Dentro de estas se puede destacar la aplicación Antares, la cual se encarga de mostrar un mapa de posición de las unidades subordinadas.

Cada servidor está incluido en una máquina virtual, dando servicio a las tres aplicaciones que se han definido en el apartado 2.1 del Análisis del Sistema:

1. El servidor Microsoft Exchange da servicio a las aplicaciones de mensajería.
2. El servidor Microsoft SharePoint da servicio a las aplicaciones de gestión táctica, principalmente mediante la creación de páginas web.
3. El servidor SIMACET da servicio a las aplicaciones de gestión táctica y de información geográfica, ambas incluidas en el propio software de SIMACET.

Cabe destacar que si fuera necesario crear máquinas virtuales adicionales, se podría hacer, además de poder aumentar o modificar los recursos de una ya creada. Como puede verse, la virtualización proporciona flexibilidad en la creación de redes.

En cuanto al reparto de recursos (memoria RAM y almacenamiento) entre las máquinas virtuales, se va a realizar de la siguiente manera, por normal general:

- Controlador de dominio: un sexto de los recursos disponibles.
- Microsoft Exchange: dos sextos de los recursos disponibles.
- Microsoft SharePoint: un sexto de los recursos disponibles.
- SIMACET: dos sextos de los recursos disponibles.

Esta decisión está basada en el hecho de cuáles son los dos servicios que más utilizan los usuarios y que más recursos precisan, en este caso el posicionamiento de unidades en SIMACET y el servicio de correo electrónico.

Según “Anexo F: Creación de máquina virtual en VMware”, se establecen los pasos necesarios para la creación de una máquina virtual en VMware Workstation Pro con Windows Server 2012 R2.

4.3 Instalación de Windows Server 2012 R2

La base para crear las cuatro máquinas virtuales, establecidas en el apartado anterior, es una máquina virtual de Windows Server 2012 R2, y por ello, la instalación más importante. Para llevarla a cabo, se ha configurado con 2 GB de RAM y 60 GB de almacenamiento. Con el fin de no cometer ningún error en la instalación de esta, se procede a la explicación de los puntos más importantes, estando el resto de pasos detallados y expuestos en capturas de pantalla en el Anexo F:

1. Cuando se configura el disco duro de la máquina virtual se debe seleccionar si se desea que este se cree sobre un solo archivo o sobre varios. El objetivo de este punto es facilitar el movimiento de la máquina virtual a otro ordenador, mediante la selección de crear el disco duro en varios archivos. En el presente trabajo se va a

crear en un solo disco, puesto que no se tiene previsto su uso en otros ordenadores, además de que ocupa menos espacio en el disco duro.

2. Una vez se inicia el asistente de configuración de Windows Server se debe elegir adecuadamente el Sistema operativo que se desea instalar. Para una instalación de los elementos necesarios para la utilización del servidor se debe elegir la opción "Server Core".

4.4 Instalación Active Directory Domain Server

Una vez se ha terminado la instalación de Windows Server se procede a la Instalación del controlador de dominio (Active Directory Domain Server). Esta es la instalación que reviste mayor dificultad, por lo que en este apartado se van a explicar los puntos más importantes a tener en cuenta, los cuales están detallados con capturas de pantalla en el Anexo G.

A continuación se van a exponer los puntos más importantes a tener en cuenta:

1. Las configuraciones iniciales deben de realizarse antes de iniciar el proceso de instalación. Estas configuraciones son el direccionamiento IP del equipo, que debe estar acorde al direccionamiento de la red, y el nombre de equipo, que el hecho de cambiarlo facilita el trabajo a posteriori. En cuanto al direccionamiento, en el manual se han establecido los siguientes valores, que dependiendo de la red, pueden variar:

   - Dirección IP: 192.168.50.1
   - Máscara de subred: 255.255.255.0
   - Puerta de enlace predeterminada: 192.168.50.254
   - Servidor DNS: 192.168.50.1

2. En el punto 5 del Anexo G hay que elegir los roles y características que se desean instalar. Este paso es el más importante, puesto que hay que marcar exactamente los roles y características que son necesarios, dado que la falta de un rol o una característica provocará que el controlador de dominio esté incompleto y no funcione correctamente.
3. En el momento previo a promover el servidor a controlador de dominio se debe acceder al equipo como el usuario "Administrator" que el equipo crea por defecto. Si no se realiza este paso la instalación da un fallo y no deja completarla. Este punto se corresponde con el paso 10.
4. La creación de un nuevo bosque[11] es esencial si no se dispone de uno creado previamente. Para cada ejercicio militar se crea uno nuevo, por lo que en la configuración se debe seleccionar la opción "Agregar un nuevo bosque". Este punto se corresponde con el paso 11.

[11] Se define bosque como colección de uno o más dominios que comparten una misma estructura lógica, catálogo global, esquema y configuración.

4.5 Instalación Microsoft Sharepoint y Microsoft Exchange

Ambas instalaciones se realizan sobre una máquina virtual de Windows Server 2012 R2, previamente clonada[12] de la máquina virtual original de Windows Server.

Para llevar a cabo el proceso, se ejecuta el software de cada herramienta en la máquina virtual mencionada, siguiendo el asistente de instalación hasta su finalización. Dado que la instalación de ambos no reviste ninguna dificultad, no se va a incluir manual de estas en los anexos.

4.6 Instalación software de SIMACET

La instalación del software que contiene las aplicaciones propias de SIMACET se realiza directamente en una máquina virtual de Windows Server 2012 R2. El proceso de instalación no reviste dificultad. Añadir, que tras la instalación de este, en el escritorio de la máquina virtual de Windows Server, utilizada para albergar este software, se muestra la aplicación Cancerbero, la cual es el menú que muestra todas las aplicaciones propias de SIMACET.

Por ser un software militar del Ejército de Tierra, que contiene información clasificada, no puede ser mostrado como tal en esta memoria.

4.7 Comprobaciones realizadas

Para las comprobaciones oportunas se ha utilizado como host anfitrión un ordenador personal con 4 GB de RAM, 111 GB de almacenamiento y Windows 10 Home como Sistema operativo anfitrión, resultando todas ellas satisfactorias:

- Comprobación 1: con la creación de discos duros dinámicos se ocupa solo los Gigabytes que realmente se están utilizando, no toda la capacidad que se asigna a cada VM, en este caso 60 GB. Esto permite hacer un uso eficiente de los recursos hardware disponibles.
- Comprobación 2: inicio de cada una de las VM, y más concretamente el acceso a la aplicación Cancerbero, la cual se sitúa en la máquina virtual de SIMACET y agrupa al resto de aplicaciones del Sistema. Este paso es esencial para poder acceder al mapa de posicionamiento de unidades en la aplicación Antares.
- Comprobación 3: creación de usuarios y unidades organizativas (UO)[13] en la máquina virtual de controlador de dominio. Este es un paso esencial en la configuración avanzada del nodo.
- Comprobación 4: creación de dos usuarios en la máquina virtual Exchange y el envío de correos electrónicos entre estos.

---

[12] Cuando se habla de clonar una máquina virtual se refiere a la herramienta que permite hacer una copia exactamente igual a la primera, pero con identidad diferente.

[13] Carpetas que se crean para la organización de los usuarios del dominio

5. Análisis de riesgos

Tal y como se ha mencionado en el apartado 1.1 “Objetivos y Alcance”, para realizar el análisis de riegos del nodo virtualizado se va a utilizar la metodología MAGERIT v3 (6), explicada en tres documentos: Libro I “Método” (7), Libro II “Catalogo de Elementos” (8) y Libro III “Guía de Técnicas” (9).

Para ello, la mencionada metodología establece las siguientes etapas a desarrollar en el análisis de riesgos:

1. Definición del contexto.
2. Valoración de los activos.
3. Análisis de las amenazas.
4. Estimación del riesgo potencial.
5. Elección de salvaguardas.
6. Estimación del riesgo residual.

Dado que el objetivo final de este trabajo es servir como base para la aplicación de la virtualización a los Sistemas de Información militares, y teniendo en cuenta la limitación de la extensión de la memoria, se van a realizar los tres primeros puntos de la metodología junto con el punto 5, elección de salvaguardas. Aclarar que este análisis conforma una primera iteración del mismo, siendo los primeros pasos, explicados en esta memoria, los más complejos en el inicio del análisis, y que servirían como base de un futuro análisis más detallado.

Para la realización del análisis se han tenido en cuenta los conceptos adquiridos en el periodos de prácticas externas en Ceuta, junto con la experiencia propia y la asignatura de SIMACET impartida en la Academia de Ingenieros.

Con el objetivo de que cada una de los puntos explicados sea de fácil comprensión se va a aplicar la siguiente estructura: en primer lugar se explica en qué consiste cada etapa o punto, para a continuación aplicarla al Sistema trabajado. Para ello, las explicaciones se van a apoyar en la modelización del Sistema en la aplicación PILAR (10), la cual fue creada para permitir una realización del análisis más organizada y visual.

5.1 Definición del contexto

El contexto define el escenario en que va a operar el Sistema de Información, siendo SIMACET en este caso:

1. La información clasificada que maneja.
2. Los servicios que proporciona.

A continuación se exponen las dos características principales del escenario.

5.1.1 La información clasificada que maneja

Esta es una de las características más importantes a tener en cuenta en un Sistema de Información militar, puesto que gran parte de la información con la que se

trabaja está clasificada, ya sea a nivel nacional o internacional, normalmente a nivel OTAN[14].

Por un lado, la seguridad en SIMACET implementa información clasificada, lo que implica la utilización de las guías de seguridad CCN-STIC[15] (11) del Centro Criptológico Nacional, además de la imposibilidad de incluir en esta memoria la información incluida en estas guías.

Por otro lado, gran parte de la información con la que trabajan los usuarios de una red SIMACET está también clasificada, puesto que en cualquier ejercicio táctico o en una misión en el exterior se trabaja con este tipo de información.

5.1.2 Los servicios que proporciona

Un nodo SIMACET proporciona básicamente tres servicios a los cuales accederán la mayor parte de los usuarios de este:

1. Servicio de correo electrónico.
2. Servicio de compartición de archivos.
3. Servicio de posicionamiento de unidades subordinadas.

Puesto que estos tres servicios requieren unos recursos adecuados al importante uso que se les da, 2 de las 4 máquinas virtuales que se crean son exclusivas para correo electrónico por un lado (Windows Exchange Server), y compartición de archivos por otro (Windows SharePoint Server), tal y como se ha explicado en el apartado 4.2.

Para el posicionamiento de unidades, el propio SIMACET incluye la aplicación Antares que permite visualizar la posición de las unidades subordinadas en un mapa de situación.

Como puede observarse en la figura 5.1, la topología inicial del diseño de la red consiste en que mediante direccionamiento IP y a través de un router[16], los usuarios del Sistema se conecten al host físico, y de esta forma, acceder a los servicios mencionados en este apartado. Aunque no se ha tenido en cuenta, y si la situación lo requiere, se podrían configurar los correspondientes switches[17], situándose estos entre los PCs de usuario y el router.

---

[14] En ejercicios tácticos combinados con países OTAN se utiliza la clasificación de información que establece tal Organización, similar a la establecida a nivel nacional, detallada en Anexo D.

[15] Las guías CCN-STIC son una serie de recomendaciones y manuales que el Centro Criptológico Nacional ha establecido para su aplicación en Sistemas de Información de la Administración Pública. Estas guías están centradas tanto en la seguridad de los Sistemas, como en Normas, Procedimientos o en la realización de análisis de riesgos.

[16] Dispositivo que proporciona conectividad a nivel de red o nivel 3 en el modelo OSI, es decir, permite que los usuarios se conecten a la red. Encamina a través de direcciones IP.

[17] Dispositivo que permite conectar dos o mas segmentos de red, situado en el nivel 2 en el modelo OSI. Encamina a través de direcciones MAC.

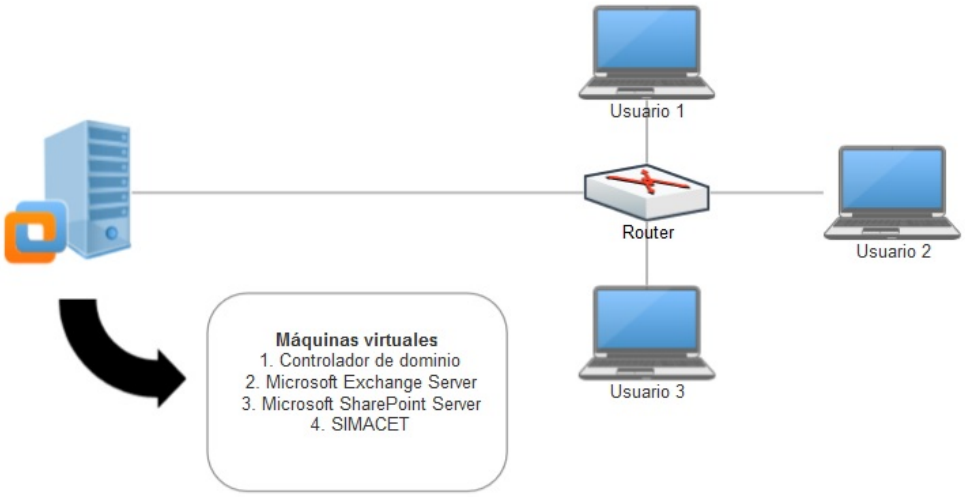


Figura 5.1 Topología de red inicial
Fuente: elaboración propia

5.2 Valoración de los activos

El manual de Magerit v3, Libro I, define activo como: "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos."

En este paso, la metodología establece tres actividades a realizar:

1. Inventariar activos.
2. Estudiar las dependencias entre los activos.
3. Valorar cada activo

5.2.1 Inventariar activos

En primer lugar se diferencia entre activos esenciales y activos relevantes. Dentro del primer grupo nos encontramos con:

- Información clasificada.
- Servicios que se prestan.

Dentro del segundo grupo nos encontramos diferentes tipos de activos[18] como:

- Aplicaciones (software).
- Equipos informáticos (hardware).
- Equipamiento auxiliar.
- Instalaciones físicas.
- Personal.

[18] Los tipos de activos se detallan en el capítulo 2 del Libro II "Catálogo de Elementos".

Tras un detallado estudio del Sistema y de los activos que le afectan, se obtiene la identificación de activos que se muestra a continuación. Como puede observarse, al introducirlos y configurarlos en la aplicación PILAR hay que diferenciarlos en activos esenciales y activos relevantes, y en el tipo que es cada uno (esenciales, equipamiento, instalaciones o personal), obteniendo la distribución que se muestra en la figura 5.2

Cada activo conlleva una caracterización según el catalogo de elementos de la metodología Magerit (8).

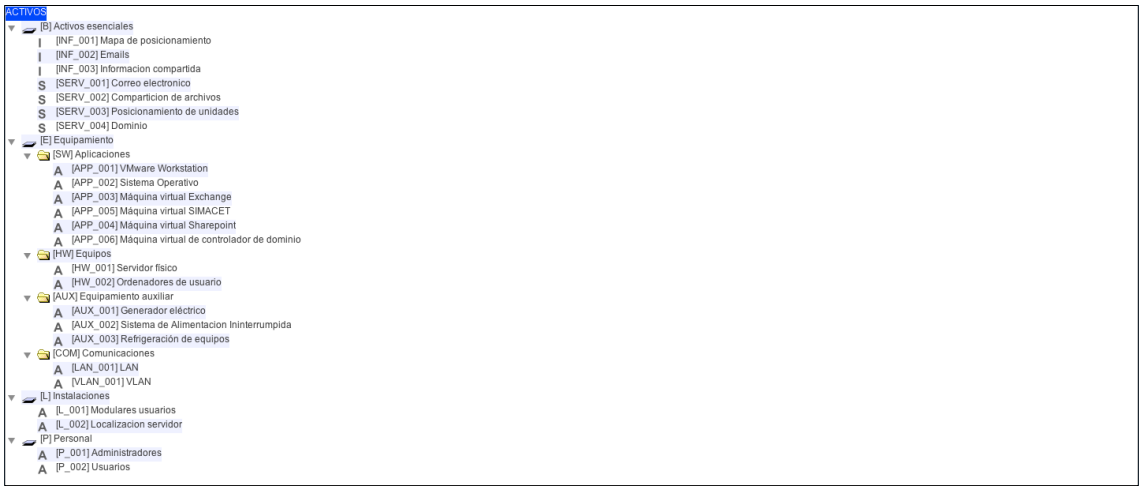


Figura 5.2 Identificación de activos
Fuente: elaboración propia

5.2.2 Dependencias entre activos

La dependencia entre activos supone que en el caso de que una amenaza que afecte a un activo del que dependa otro activo superior, tendrá impacto directo sobre el activo superior, es decir, el fallo de un activo subordinado afecta directamente al activo inmediatamente superior.

Para entender mejor las dependencias entre los activos, identificados en la fase anterior, como fruto del estudio del Sistema, se van a exponer en un diagrama de bloques que muestre de una forma más visual las dependencias existentes entre estos. Este diagrama es generado por la propia aplicación PILAR tras establecer las dependencias entre cada activo obtenidas en el estudio del Sistema mencionado en el apartado anterior.

El diagrama presentado es el correspondiente al diagrama de buses, generado dentro del apartado mencionado en el párrafo anterior. La elección de este se basa únicamente en el hecho de que es el diagrama que mejor estructura y visualiza las dependencias entre activos.

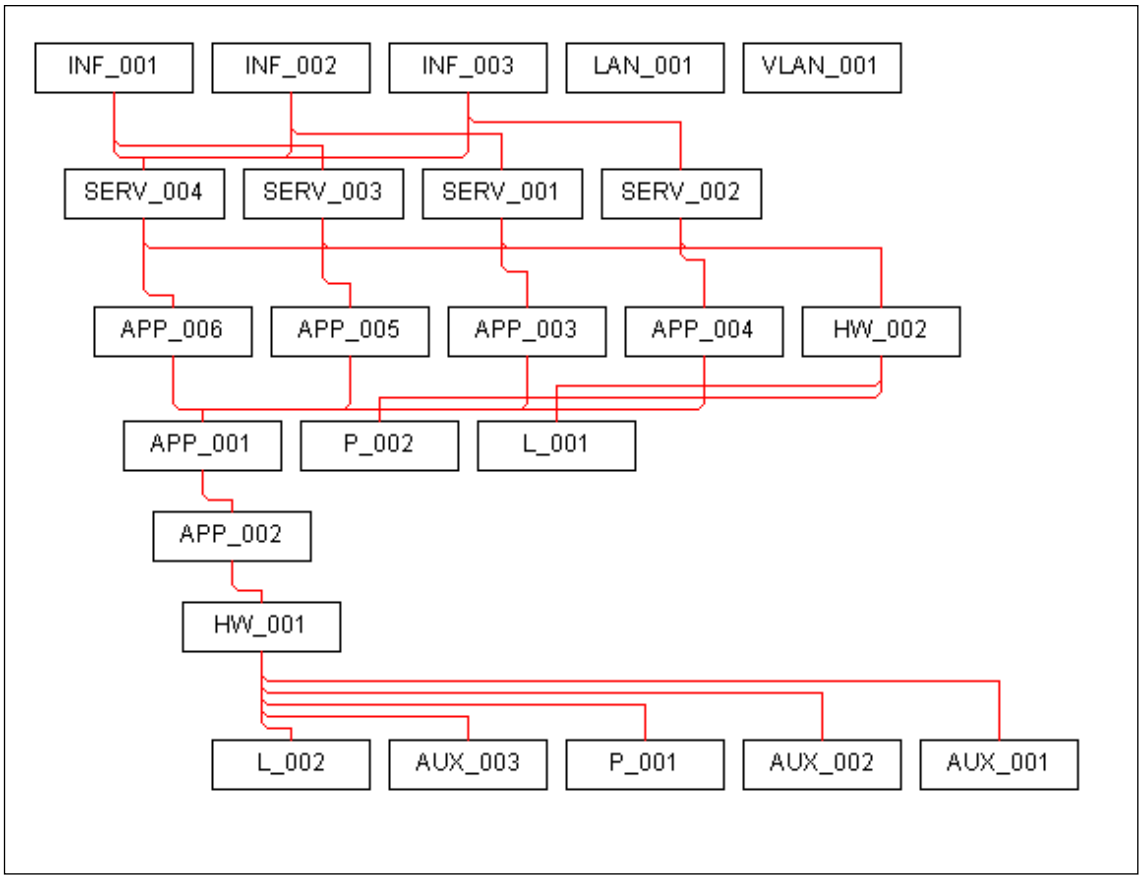


Figura 5.3 Dependencias entre activos
Fuente: elaboración propia

La estructura básica de dependencia de activos sitúa a la Información como activo principal, del cual cuelgan el resto de activos. En segundo lugar, se sitúan los Servicios prestados, seguidos de Software y Equipamiento. En este caso, la estructura básica queda de la siguiente forma:

1. Información (INF_001, INF_002 e INF_003).
2. Servicios (SERV_001, SERV_002, SERV_003 y SERV_004).
3. Máquinas virtuales (APP_003, APP_004, APP_005 y APP_006).
4. Software de virtualización (APP_001).
5. Sistema operativo del host anfitrión (APP_002).
6. Servidor físico (HW_001).

Teniendo en cuenta que esta estructura está marcada por la metodología MAGERIT, se procede a explicar las dependencias más importantes:

1. Dependencias Información-Servicios: la Información es el activo más importante, creada en los servicios y gestionada dentro de estos. Por ello, un mínimo fallo en un servicio podría generar una vulnerabilidad en los activos INF_001, INF_002 e INF_003. Por ejemplo, un fallo en el servicio de dominio afectaría directamente a los tres activos de Información, tal y como se ha modelado en la figura 5.3. Además, un activo Información puede tener

dependencias con varios activos Servicio, aumentando más aún las posibilidades de ocurrencia de vulnerabilidades.

2. Dependencias Servicios-Máquinas virtuales: cada activo Servicio esta implementado en una máquina virtual, es decir, en un activo de tipo Aplicaciones. Esto implica que un error en una VM afecte a un Servicio, pudiendo llegar a detenerlo.

3. Dependencias Máquinas virtuales-SW virtualización: cada VM está creada y gestionada por el software de virtualización, lo que obliga a que los activos APP_003, APP_004, APP_005 y APP_006 tengan una dependencia directa con el activo APP_001.

4. Dependencia SW virtualización-Sistema Operativo: al ser hipervisor tipo 2, el software de virtualización se instala sobre un Sistema Operativo, lo que hace necesaria la dependencia entre ambos, en este caso entre APP_001 y APP_002.

5. Dependencia Sistema Operativo-Servidor físico: el activo APP_002 (Sistema Operativo) se instala sobre el servidor físico, activo HW_001, lo que implica la dependencia directa entre ambos.

Por otro lado, el servidor físico tiene dependencia directa con todos los elementos que conforman el equipamiento auxiliar, es decir, con los activos AUX_001, AUX_002 y AUX_003. Dichos activos son realmente importantes para la red, puesto que son los encargados de proporcionar la electricidad necesaria para su correcto funcionamiento.

Es necesario también nombrar los activos que conforman al personal que va a gestionar, por un lado, y explotar, por otro, el Sistema de Información. En este punto, se ha de destacar que los Administradores (activo P_001) tienen dependencia directa con el servidor físico, el cual gestionan, y los Usuarios (activo P_002) tienen dependencia directa con los Ordenadores de Usuario (HW_002), a través de los cuales explotan los servicios del Sistema.

Se debe tener en cuenta que los activos que se encuentran en la parte superior se ven afectados por los posibles incidentes que les ocurran a los activos situados en la parte inferior del diagrama. Teniendo en cuenta esto y como ejemplo, cualquier fallo en alguno de los servicios que se prestan, en el servidor físico o en el software de virtualización VMware Workstation, repercutiría directa o indirectamente en los activos esenciales de tipo Información.

Cabe destacar que todos los activos que se han identificado no se han tenido en cuenta en el diagrama de dependencia de los mismos. En este caso, los activos incluidos en “Comunicaciones” no se han incluido en el diagrama de dependencias, simplemente se han identificado, dado que las comunicaciones dentro de SIMACET no son objeto de este trabajo.

5.2.3 Valoración de los activos

En el momento de la valoración de los activos, esta se debe hacer conforme a una o varias dimensiones de seguridad. Se entiende por dimensión de la seguridad el enfoque que posteriormente se le dará a la securización del sistema. Dichas dimensiones se muestran en la tabla siguiente:

Disponibilidad	Las personas y/o procesos autorizados tienen acceso al sistema cuando lo requieren
Integridad	El sistema no ha sido modificado de manera no autorizada
Confidencialidad	La información está disponible únicamente para las personas y/o procesos autorizados
Autenticidad	Garantía de la fuente de la que proceden los datos o información
Trazabilidad	Las actuaciones de una persona y/o proceso pueden ser imputadas exclusivamente a dicha persona y/o procesos

Tabla 5.1 Dimensiones de seguridad
Fuente: elaboración propia

El presente trabajo se va a realizar conforme a la dimensión de seguridad disponibilidad, puesto que esta es un requisito de los Sistemas de Información en el Ejército de Tierra, asegurando el acceso a los Sistemas en cualquier momento de una operación militar.

Además, también se va a realizar conforme a la dimensión de seguridad confidencialidad, siendo esta imprescindible en el montaje de redes para puestos de mando del Ejército de Tierra.

Por otro lado, el análisis se puede realizar de forma cualitativa o cuantitativa, siendo la primera opción la elegida para el presente trabajo. Para ello, el análisis se basa en una escala de valores del 0 al 10, siendo 0 un valor que no reviste preocupación y 10 un valor totalmente inaceptable.

La valoración de los activos se ha realizado conforme a las indicaciones y entrevistas realizadas a personal de la Compañía de Transmisiones 17 de Ceuta. Además, personal de la Academia de Ingenieros (ACING) situada en Hoyo de Manzanares, ha sido también de gran ayuda en la realización de la misma. Se ha de tener en cuenta que en un Sistema de Información militar, como es el caso, los activos se van a valorar de forma diferente a como se haría en un Sistema del ámbito civil, dado que las necesidades, tanto de información como de servicios, son muy diferentes.

En primer lugar, es necesario valorar los activos esenciales, los cuales determinarán la valoración de los activos relevantes. A continuación, en la figura 5.4, se muestra la valoración inicial mencionada al inicio del párrafo:

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
I [INF_001] Mapa de posicionamiento			[7]
I [INF_002] Emails			[7]
I [INF_003] Informacion compartida			[9]
S [SERV_001] Correo electronico	[7]		
S [SERV_002] Comparticion de archivos	[5]		
S [SERV_003] Posicionamiento de unidades	[9]		
S [SERV_004] Dominio	[7]		

Tabla 5.2 Valoración de activos esenciales
Fuente: elaboración propia

Tal y como ha sido mencionado con anterioridad, el análisis de riesgos se va a centrar en dos dimensiones: disponibilidad y confidencialidad. En el primer caso, se van a valorar los activos que forman los Servicios; en el segundo caso, se van a valorar los activos que forman la Información.

Los criterios[19] que se han seguido para los activos SERV_00X han sido los establecidos para posibles interrupciones del servicio.

En el caso del activo SERV_001, se valora con el criterio [7.da] puesto que el servicio de correo electrónico se considera imprescindible. Además, la carencia de este podría causar un impacto significativo en otras Organizaciones, en este caso unidades militares, tanto subordinadas como adyacentes.

El activo SERV_002 se valora con el criterio [5.da] dado que no se considera un servicio imprescindible, pudiendo conducir una operación militar sin el uso de herramientas de Sharepoint.

Los activos SERV_003 y SERV_004 se valoran con el criterio [9.da]. Esta decisión está basada en los siguientes puntos:

1. El posicionamiento de unidades subordinadas es un servicio imprescindible para el Jefe de la Gran Unidad. La carencia de este provocaría la imposibilidad de dirigir una operación militar adecuadamente.
2. El controlador de dominio es fundamental en el establecimiento de una red de SIMACET.

Los criterios que se han seguido para los activos INF_00X han sido los establecidos para seguridad, información clasificada e información personal.

Los tres activos de Información han sido valorados con el criterio [7.lbl] puesto que la mínima clasificación de la información que se establece en un puesto de mando es Confidencial.

Los activos INF_001 e INF_002 han sido valorados con el criterio [7.si] de seguridad dado que una carencia en la seguridad de esta información podría provocar un grave incidente de seguridad. Esto se justifica con el tipo de información delicada que estos servicios tratan: posicionamiento de unidades y emails. Además, el activo INF_002 ha sido también valorado con el criterio [6.pi2] por la posibilidad de que en algún email adjunte información personal de algún integrante del puesto de mando.

Por último, el activo INF_003 ha sido valorado con el criterio [9.si] por la información que se pueda compartir mediante herramientas de Sharepoint, la cual podría estar clasificada y compartida únicamente para cierto personal, provocando la filtración de esta un serio incidente de seguridad.

La aplicación PILAR, teniendo en cuenta la valoración que se haya hecho de los activos esenciales genera valoraciones para el resto de activos, atendiendo al diagrama de dependencias que se haya diseñado. Por ello, la tabla final de valoraciones queda de la siguiente manera:

[19] La lista completa de criterios establecidos se muestra en el Anexo H

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[INF_001] Mapa de posicionamiento			[7]
[INF_002] Emails			[7]
[INF_003] Informacion compartida			[9]
[SERV_001] Correo electronico	[7]		[7]
[SERV_002] Comparticion de archivos	[5]		[9]
[SERV_003] Posicionamiento de unidades	[9]		[7]
[SERV_004] Dominio	[7]		[9]
[E] Equipamiento			
[SW] Aplicaciones			
[APP_001] VMware Workstation	[9]		[9]
[APP_002] Sistema Operativo	[9]		[9]
[APP_003] Máquina virtual Exchange	[7]		[7]
[APP_005] Máquina virtual SIMACET	[9]		[7]
[APP_004] Máquina virtual Sharepoint	[5]		[9]
[APP_006] Máquina virtual de controlador de dominio	[7]		[9]
[HW] Equipos			
[HW_001] Servidor físico	[9]		[9]
[HW_002] Ordenadores de usuario	[9]		[9]
[AUX] Equipamiento auxiliar			
[AUX_001] Generador eléctrico	[9]		
[AUX_002] Sistema de Alimentacion Ininterrumpida	[9]		
[AUX_003] Refrigeración de equipos	[9]		
[COM] Comunicaciones			
[LAN_001] LAN			
[VLAN_001] VLAN			
[L] Instalaciones			
[L_001] Modulares usuarios	[9]		[9]
[L_002] Localizacion servidor	[9]		[9]
[P] Personal			
[P_001] Administradores	[9]		[9]
[P_002] Usuarios	[9]		[9]

Tabla 5.3 Valoraciones acumuladas de activos[20]
Fuente: elaboración propia

Observando las valoraciones acumuladas, se obtienen ciertas conclusiones. En primer lugar, la importancia del activo SERV_003 en la dimensión disponibilidad, de los activos SERV_002 y SERV_004 en la dimensión confidencialidad, de los activos que definen a las VMs (APP_003, APP_004, APP_005 y APP_006) y por ende, los activos APP_001 y APP_002. En este punto se debe destacar la importancia del activo del software de virtualización (APP_001), el cual, situado entre el host físico y el Sistema operativo (en el diagrama de dependencias) tiene un papel fundamental en la creación y gestión de las máquinas virtuales. Como se puede observar, la importancia de cada activo superior define claramente la importancia de los activos subordinados, teniendo en cuenta la distribución de estos en el diagrama de dependencias de activos. Por ejemplo, el activo SERV_003 en la dimensión disponibilidad tiene una valoración de 9, que se extiende a la máquina virtual subordinada (SERV_005) con un 9, y a los activos APP_001 y APP_002 con un 9 en ambos.

Se debe tener en cuenta, que estas valoraciones se deberían de tomar como punto inicial para el desarrollo del trabajo que en esta memoria se explica, puesto que podrían incluirse más activos, modificando de esta forma, la identificación de activos y las dependencias entre estos.

5.3 Análisis de las amenazas

Los activos están expuestos a amenazas, las cuales pueden provocar una cierta degradación de estos. Para conocerlas y evitarlas, la aplicación PILAR facilita una serie de herramientas con el fin de obtener unos datos que faciliten la securización del Sistema. Para ello, la aplicación propone una serie de amenazas que junto con los valores numéricos, escalados por

[20] Para su correcta visualización se incluye una copia del mismo en Anexo I.

la metodología, de probabilidad de ocurrencia y degradación de los activos, muestra visualmente el impacto de cada amenaza. La aplicación PILAR utiliza las siguientes escalas:

Nivel	Porcentaje
Total	100 %
Muy alta	90 %
Alta	50 %
Media	10 %
Baja	1 %

Tabla 5.4 Escala de degradación de activos
Fuente: elaboración propia

Nivel	Frecuencia
Muy alto	100
Alto	10
Medio	1
Bajo	0,1
Muy bajo	0,01

Tabla 5.5 Escala de probabilidad de ocurrencia
Fuente: elaboración propia

Las tablas muestran los valores que la metodología da a las dos escalas mencionadas. En la tabla 5.4 se escala la degradación que sufre el activo en tanto por ciento, mientras que la tabla 5.5 muestra la probabilidad de ocurrencia de las amenazas que se hayan identificado.

Para que sirva como base de un futuro desarrollo del presente trabajo, y como causa de la limitación en la extensión de la memoria, se muestran las amenazas que afectan al activo HW_001 “Servidor físico” en la figura 5.6. La primera valoración es la probabilidad de ocurrencia, cuyos valores se sitúan entre 0,01 y 100. La segunda valoración, dada para cada dimensión (a la izquierda, disponibilidad; a la derecha, confidencialidad), tiene unos valores que se sitúan entre 1% y 100%. En el caso que se muestra, la amenaza [E.24] “Caída del sistema por agotamiento de recursos” sería la amenaza mas importante a tener en cuenta, mientras que, la amenaza [N. 2] “Daños por agua” sería a la que menos importancia habría que darle.

A continuación se muestra los valores que la propia aplicación PILAR da a cada uno de los dos factores a tener en cuenta:

activo	frecuencia	[D]	[I]	[C]
ACTIVOS				
[B] Activos esenciales				
[E] Equipamiento				
[SW] Aplicaciones				
[HW] Equipos				
[HW_001] Servidor físico		100%		100%
[N.1] Fuego	0,1	100%		
[N.2] Daños por agua	0,1	50%		
[N.*] Desastres naturales	0,1	100%		
[I.1] Fuego	0,5	100%		
[I.2] Daños por agua	0,5	50%		
[I.*] Desastres industriales	0,5	100%		
[I.3] Contaminación medioambiental	0,1	50%		
[I.4] Contaminación electromagnética	1	10%		
[I.5] Avería de origen físico o lógico	1	50%		
[I.6] Corte del suministro eléctrico	1	100%		
[I.7] Condiciones inadecuadas de temperatura o humedad	1	100%		
[I.11] Emanaciones electromagnéticas	1			1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware	1	10%		
[E.24] Caída del sistema por agotamiento de recursos	10	50%		
[E.25] Pérdida de equipos	0,1	100%		100%
[A.7] Uso no previsto	1	1%		10%
[A.11] Acceso no autorizado	1	10%		50%
[A.23] Manipulación del hardware	0,5	50%		50%
[A.24] Denegación de servicio	2	100%		
[A.25] Robo de equipos	0,1	100%		100%
[A.26] Ataque destructivo	1	100%		

Tabla 5.6 Valoraciones acumuladas de amenazas[21]
Fuente: elaboración propia

La aplicación identifica y valora amenazas de toda índole, es decir, desde el punto de vista de las instalaciones físicas del puesto de mando, a cualquier tipo de ataque al Sistema tanto por un usuario interno al mismo, como por un usuario externo.

Pese a que a priori pueda parecer que se dan unas valoraciones muy altas, esto sucede como causa de la necesidad de crear redes muy robustas, que permitan el funcionamiento de unos servicios determinados en cualquier situación.

5.4 Elección de salvaguardas

Tras la identificación de las amenazas, la aplicación PILAR muestra un conjunto de salvaguardas para la securización del conjunto del Sistema. Dichas salvaguardas están enfocadas a todo el conjunto de activos que se han determinado, facilitando de esta forma, la identificación y solución de cualquier vulnerabilidad que afecte al Sistema analizado en su conjunto.

En el caso que se analiza en esta memoria, la aplicación ha generado el conjunto de salvaguardas que se muestra en la figura 5.7, cada una con los sub-apartados determinados y una valoración de la importancia de estas. Para la correcta visualización y comprensión de todas las salvaguardas, se incluye una copia de cada una de estas en el Anexo K.

Como puede observarse en la figura 5.7, las salvaguardas mas valoradas son:

1. [SW] “Protección de las Aplicaciones Informáticas” con 7.
2. [HW] “Protección de los Equipos Informáticos” con 7.
3. [L] “Protección de las instalaciones” con 7.
4. [tools] “Herramientas de seguridad” con 8.

[21] Para su correcta visualización se incluye una copia del mismo en Anexo J.

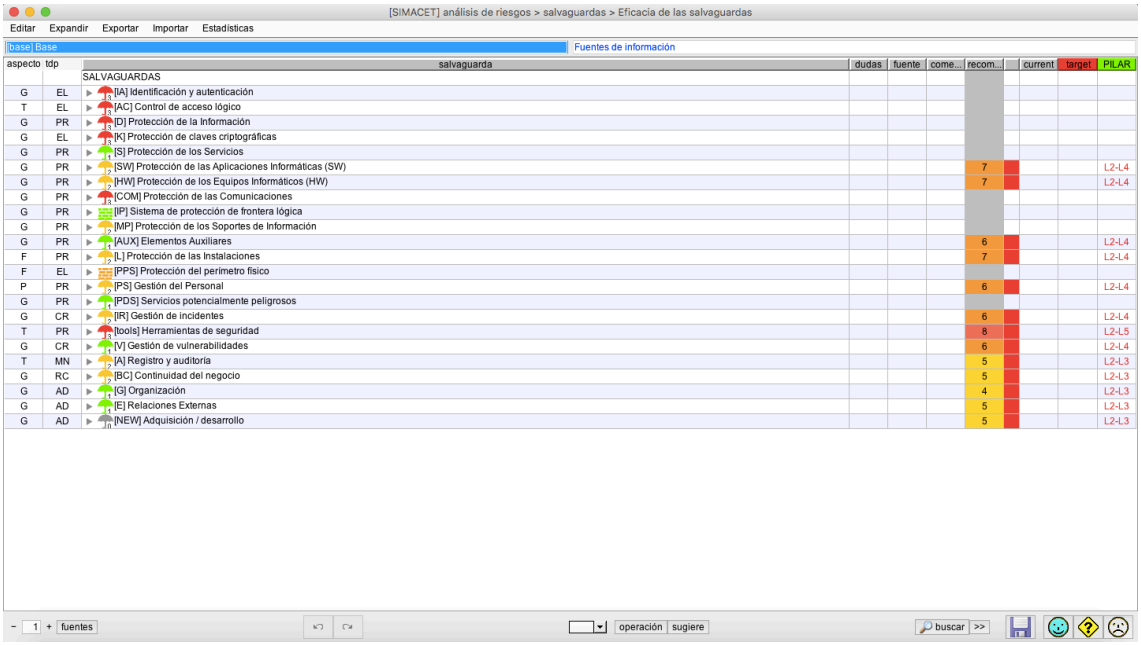


Tabla 5.7 Valoración de salvaguardas[22]
Fuente: elaboración propia

Como puede observarse, la securización del nodo en todos los ámbitos es esencial, desde el software, al hardware y a las instalaciones. Más concretamente, las herramientas de seguridad, deberían tener un valor importante en siguientes iteraciones del análisis de riesgos.

6. Análisis de ventajas y desventajas de la virtualización

Tras la realización de las instalaciones correspondientes y el análisis de riesgos, se han obtenido una serie de conclusiones que conforman las ventajas y desventajas de utilizar la tecnología de virtualización, las cuales se muestran a continuación:

6.1 Ventajas de la virtualización

La tecnología de virtualización posee un amplio abanico de ventajas, las cuales van a ser expuestas a continuación:

- Aislamiento: cada máquina es independiente de las otras, por lo que si una VM falla, no afectará a las demás máquinas virtuales, las cuales seguirán funcionando adecuadamente. Por otro lado, una vulneración de seguridad en una máquina tampoco afectará a la seguridad de las demás. En un nodo SIMACET, si una de las máquinas se "corrompe" o falla, no afectará a las demás ni en los archivos que contiene ni en la configuración realizada.

- Flexibilidad: se pueden crear las VM con la CPU, memoria, disco y red que se quiera, dentro de un mismo host físico. Esta ventaja permite, además, tener diferentes sistemas operativos en diferentes máquinas virtuales, siendo ejecutadas desde un mismo software de virtualización y al mismo tiempo. Esta ventaja permite

[22] Para su correcta visualización se incluye una copia del mismo en Anexo K.

la modificación de la configuración de una cierta máquina si en un cierto momento esta requiere de más recursos.

- Agilidad: el proceso de creación de una VM es rápido, facilitando de esta forma, la creación de las máquinas virtuales que se necesiten, teniendo como único límite los recursos que el host físico puede ofrecer a los host virtuales. Como puede comprobarse en los manuales incluidos en los anexos, el proceso de creación de una máquina virtual no requiere de mucho tiempo.

- Portabilidad: toda la configuración de una máquina virtual se encuentra en una serie de archivos, los cuales pueden ser copiados de forma sencilla y rápida a otro host físico, y de esta manera, poder disponer de la VM en este otro host. Esto permite poder redundar el host anfitrión, y de esta forma poder disponer de este en caso de necesidad.

- Recuperación rápida en caso de fallo: si se dispone de los archivos que conforman la máquina virtual (que previamente deben haber sido clonados, como medida de seguridad, a través del software de virtualización), resulta fácil ejecutar la VM en otro host físico, simplemente arrancando esta desde el software de virtualización utilizado.

6.2 Desventajas de la virtualización

Pese a las ventajas mencionadas, existen ciertas desventajas que pueden poner en cuestión a la virtualización, provocando que dicha tecnología, en ocasiones, no sea la solución más adecuada para el despliegue de una red de un Sistema de Información:

- Rendimiento inferior: un host virtual no podrá alcanzar los niveles de rendimiento de un host físico, viéndose afectado como resultado de la capa de abstracción que el hipervisor crea para la gestión del hardware entre la parte física y la parte virtual. Además, el hecho de virtualizar ya está dividiendo los recursos totales disponibles de un host físico, lo que imposibilita que una máquina virtual pueda disponer de unos recursos similares.

- La avería del host físico afecta a todos los host virtuales alojados en este: puesto que el software de virtualización está instalado en el host físico, un fallo de este afectará a todas las VM creadas a través de dicho SW. Esta desventaja justifica la importancia de la dependencia entre los activos APP_001 “VMware Workstation” y APP_002 “Sistema operativo”, mencionada anteriormente en el análisis de riesgos.

- Portabilidad condicionada: la portabilidad del sistema se ve afectada por el SW de virtualización utilizado, puesto que no existe interoperabilidad entre diferentes soluciones de virtualización. Por ejemplo, una VM creada con el software de VMware no puede ser ejecutada ni en VirtualBox ni en Hyper-V.

- Probabilidad de fallo: esta es mayor en el caso de host virtuales, puesto que existe la posibilidad de que la máquina virtual se “corrompa” y falle, llegando incluso a perder la información contenida en los archivos que conforman la VM. Esta desventaja justifica la elección de la versión Pro, puesto que esta dispone de la capacidad de hacer instantáneas, volviendo a un estado anterior al del fallo.

- Desaprovechamiento de recursos: la creación de máquinas virtuales innecesarias provocan la disminución de los recursos disponibles, puesto que ocupan espacio en el disco duro, RAM y capacidad de proceso.

7. Conclusiones

Para el desarrollo del presente trabajo y consecución del objetivo marcado, crear un nodo SIMACET virtualizado y securizado, se establecieron tres tareas a realizar (manuales para la instalación de las máquinas virtuales necesarias, análisis de riesgos y análisis de ventajas y desventajas en el uso de la virtualización). De la realización de cada una de estas se han obtenido las siguientes conclusiones:

- Los manuales realizados conforman una base importante en la creación de un nodo virtualizado. Cada uno explica paso a paso como instalar el software esencial para la consecución del objetivo establecido. Como resultado, la formación del personal puede ser muy intuitiva e interactiva. Este hecho es también consecuencia de la flexibilidad que da la virtualización, permitiendo crear, modificar y eliminar las máquinas virtuales que sean necesarias, tal y como se ha puntualizado en el apartado 6.1.

- La virtualización con hipervisor de tipo 2 resulta ser mejor opción frente a hipervisor de tipo 1 por varios motivos. En primer lugar, y teniendo en cuenta que un nodo SIMACET de PU da servicios a un número reducido de usuarios, permite cubrir las necesidades de estos. En segundo lugar, el coste es menor, permitiendo su utilización a unidades del Ejército de Tierra con un menor presupuesto en este ámbito. Por último, permite gestionarse desde un ordenador personal, prescindiendo del uso de servidores, reduciendo con ello también el coste derivado de la compra de equipos, lo que evidencia los menores costes tanto en software como en hardware.
- Tal y como se establece en el apartado 1 de la memoria, este trabajo puede ser utilizado por cualquier Compañía de Transmisiones del Ejército de Tierra, aplicándolo a los Sistemas de Información de los que disponga, mas concretamente a SIMACET. Como línea futura de este punto, se propone la realización de un manual oficial a utilizar por el personal del Ejército de Tierra para el despliegue de puestos de mando con servicios virtualizados. En este caso, los anexos que conforman las guías de instalación podrían ser utilizados como base.
- Atendiendo al análisis de riesgos, quedan reflejadas ciertas vulnerabilidades del Sistema cuando se ejecuta como un servicio virtualizado. De este análisis se extraen varias conclusiones:

    1. El activo APP_001 “VMware Workstation” tiene una gran importancia, tanto en la dimensión confidencialidad como en disponibilidad, puesto que en el diagrama de dependencias se sitúa entre las máquinas virtuales y el sistema operativo del host anfitrión. Por ello, se debe asegurar el correcto funcionamiento del activo mencionado.
    2. Este análisis conforma la primera iteración del mismo, lo que implica la posible modificación del mismo en futuras iteraciones. Como consecuencia, cabe la posibilidad de añadir, suprimir o modificar activos y/o dependencias en iteraciones siguientes.

3. La salvaguarda [tools] “Herramientas de seguridad” ha obtenido una valoración de 8, siendo esta demasiado alta. Este hecho es consecuencia de la inexistencia de un antivirus o firewall en la identificación de activos. Este podría ser uno de los puntos a tener en cuenta en las futuras iteraciones mencionadas en este apartado.
4. Las salvaguardas [SW] “Protección de las Aplicaciones Informáticas”, [HW] “Protección de los Equipos Informáticos” y [L] “Protección de las Instalaciones” evidencian la necesidad de proteger la red en todos los aspectos.

Referencias

1. Sotoca, Teniente Sergio Jesús Núñez. (2015). La nube en el Ejército de Tierra. *Revista Ejército, 890*.

2. (MADOC), Mando de Adiestramiento y Doctrina. (2011). *PD1-001 "Empleo de las fuerzas terrestres"*. Granada.

3. (MADOC), Mando de Adiestramiento y Doctrina. (2009). *PD3-602 "Establecimiento y Empleo de SIMACET"*. Granada.

4. VMware. (1/3/18). Virtualization. https://www.vmware.com/es/solutions/virtualization.html].

5. VMware. (1/3/18). Workstation Pro. https://www.vmware.com/es/products/workstation-pro.html].

6. Electrónica, Consejo Superior de Administración. (2012, 1/3/18). MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información; https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WqYuwGabH-Y].

7. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*. Madrid.

8. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*.

9. Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de técnicas*.

10. (CCN), Centro Criptológico Nacional. (1/3/18). Aplicación PILAR. https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/pilar.html].

11. (CCN), Centro Criptológico Nacional. (1/3/18). Guías CCN-STIC. https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html].

12. (CCN), Centro Criptológico Nacional. (2017). Guía de Seguridad de las TIC CCN-STIC 470 "PILAR – Manual de Usuario (v 6.2)".

13. (MADOC), Mando de Adiestramiento y Doctrina. (2016). PD4-502 "Empleo de la Compañía de Transmisiones de la Brigada". Granada.

Anexo A: Redes lógicas de réplica en SIMACET

Tal y como se ha establecido en el Análisis del Sistema, este dispone de redes lógicas de réplica. Estas van a ser explicadas a continuación:

1. Red de réplica tipo IP de SIMACET

   Es aquella red que utiliza el protocolo IP para intercambiar la información táctica, es decir, utiliza direccionamiento IP.

2. Red de réplica tipo RRC de SIMACET

   Es aquella red lógica de SIMACET cuyos nodos asociados a esta emplean la RRC[23] para intercambiar la información táctica. Esto implica la creación de una serie de mallas de radios con su correspondiente documentación de indicativos militares y frecuencias a utilizar.

3. Red de réplica tipo LAN de SIMACET

   Es aquella red lógica de SIMACET donde los nodos asociados a esta emplean recursos compartidos (carpetas) para intercambiar la información táctica.

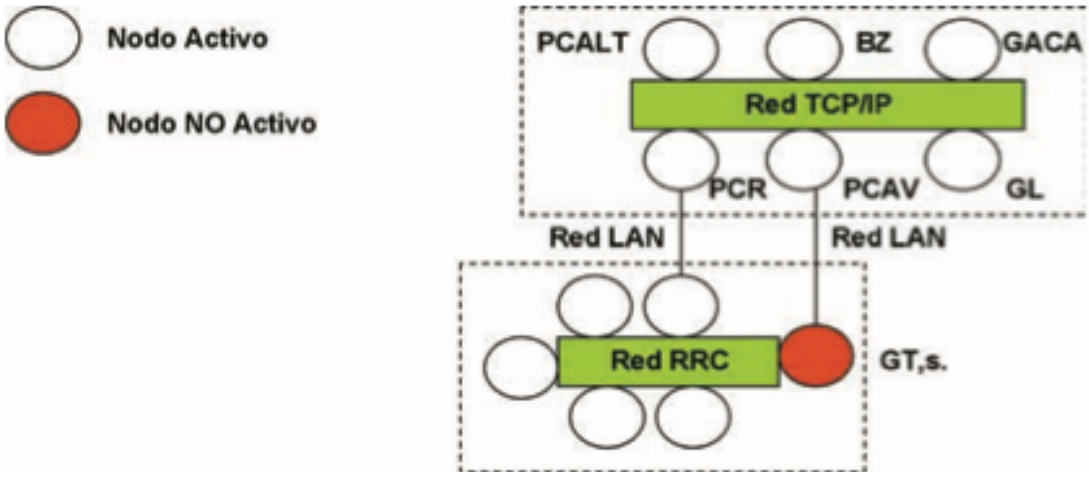


Figura A.1 Red de réplica tipo LAN
Fuente: PD3-602

En la figura A.1 se muestra como nodos de diferentes grupos de nodos están conectados mediante redes LAN. A través de estas redes y mediante unas carpetas previamente creadas, los nodos con capaces de intercambiar la información táctica. Esto permite la interconexión de diferentes redes. En este caso, mediante la Red Radio de Combate se pueda enviar la posición de ciertas unidades a un puesto de mando determinado. Esto, unido a la réplica de la base de datos, permite a los usuarios visualizar la posición de las unidades subordinadas desde diferentes ubicaciones.

[23] RRC: Red compuesta por equipos Radio que trabajan en una banda de frecuencia determinada (ej.: PR4G v3 en VHF).

Anexo B: Comparativa entre versiones de VMware Workstation

Tal y como se ha mencionado en el apartado 3.4, VMware Workstation 14 posee dos versiones con diferentes características, las cuales se comparan en la siguiente tabla:

	Workstation Player	Workstation Pro
Crear nuevas VMs	X	X
Crear VMs grandes (16 CPU y 64 GB de RAM)	X	X
Más de 200 SO invitados compatibles	X	X
Uso compartido de archivos host/ invitado	X	X
Ejecutar VMs con distintos modos de visualización	X	X
Compatibilidad con pantallas 4K	X	X
Compatibilidad con amplia gama de dispositivos virtuales	X	X
Compatibilidad con lector de tarjetas inteligentes USB	X	X
Compatibilidad con dispositivos USB 3.0	X	X
Ejecutar VMs cifradas		X
Ejecutar varias VMs al mismo tiempo		X
Crear y gestionar VMs cifradas		X
Realizar instantáneas		X
Redes avanzadas		X
Clonado de VMs		X
Conectar con servidor ESXi/vSphere		X
Operación desde la línea de comandos: vmrun		X

Tabla B.1 Comparativa de versiones VMware Workstation
Fuente: elaboración propia

Anexo C: Requisitos hardware y software de VMware Workstation 14 Pro

Tal y como se ha mencionado en el apartado 3.4, el software de virtualización VMware Workstation 14 Pro tiene unos requisitos hardware y software, los cuales se muestran a continuación:

1. Necesidades en cuanto a hardware:

- Compatibilidad con sistemas que usan procesadores (CPU) de 2011 o posterior, salvo:
  - · Procesadores Intel Atom basados en microarquitectura “Bonnell” de 2011.
  - · Procesadores Intel Atom basados en microarquitectura “Saltwell” de 2012.
  - · Procesadores AMD basados en microarquitectura “Llano” y “Bobcat”.
- Compatibilidad con sistemas que usan procesadores Intel basados en microarquitectura “Westmere” de 2010.
- Velocidad de núcleo de 1,3 GHz o superior.
- Al menos 2 GB de RAM (se recomienda 4 GB o más).

2. Sistemas operativos host anfitrión a destacar:

- Ubuntu 16.x y 17.x.
- Debian 8.9 y 9.x.
- Windows Server 2008 R2 SP1.
- Windows Server 2012, 2012 R2 y 2016.
- Windows 7, 8.x y 10.

3. Sistemas operativos invitados a destacar

- Windows Server, versiones desde 2008 hasta 2016.
- Windows XP, 7, 8.x y 10.
- Ubuntu.
- Red Hat.
- Oracle Linux.
- Debian.
- Fedora.

Anexo D: Grados de clasificación de la información según OTAN

A nivel OTAN se utiliza la siguiente clasificación de la información, la cual es similar a la utilizada en territorio nacional y que se explican y comparan a continuación:

1. COSMIC TOP SECRET: una revelación o divulgación de esta podría ocasionar un excepcional grave daño a la OTAN. A nivel nacional tiene su equivalencia en el grado SECRETO.
2. NATO SECRET: una revelación o divulgación de esta podría ocasionar un grave daño a la OTAN. A nivel nacional tiene su equivalencia en el grado RESERVADO.
3. NATO CONFIDENTIAL: una revelación o divulgación de esta podría ocasionar un daño a la OTAN. A nivel nacional tiene su equivalencia en el grado CONFIDENCIAL.
4. NATO RESTRICTED: una revelación o divulgación de esta podría ser perjudicial para los intereses de la OTAN. A nivel nacional tiene su equivalencia en el grado DIFUSIÓN LIMITADA.

A continuación se muestra una tabla comparativa de ambas clasificaciones, siendo así más visual su comparación:

NATO OTAN	COSMIC SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA

Tabla D.1 Clasificación de la información
Fuente: elaboración propia

Anexo E: Instalación de VMware Workstation 14 Pro

El Anexo D conforma la guía para la instalación del software de virtualización a utilizar, en este caso VMware Workstation Pro versión 14.

Paso 1:

En este paso simplemente se indica el software que se va a instalar en el equipo y su versión.

Figura E.1 Inicio de asistente de instalación de VMware
Fuente: elaboración propia

Para continuar se hace click sobre “Next”.

Paso 2:

En este paso es necesario aceptar los acuerdos de licencia, que previamente habrán sido leídos, para poder hacer uso del software.

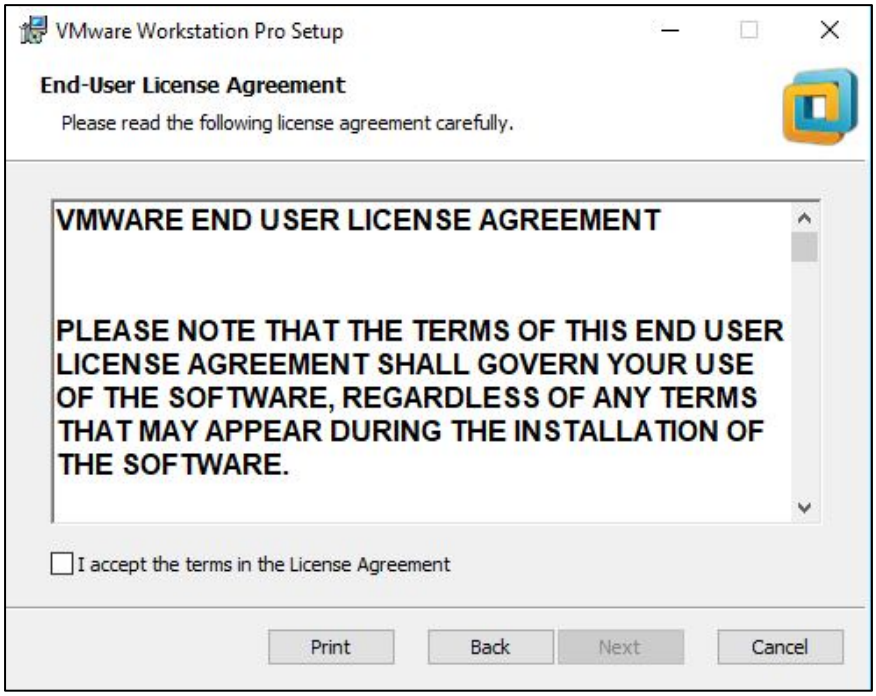


Figura E.2 Acuerdos de licencia
Fuente: elaboración propia

Tras haber leído los acuerdos se hace click sobre la pestaña que se indica a continuación:

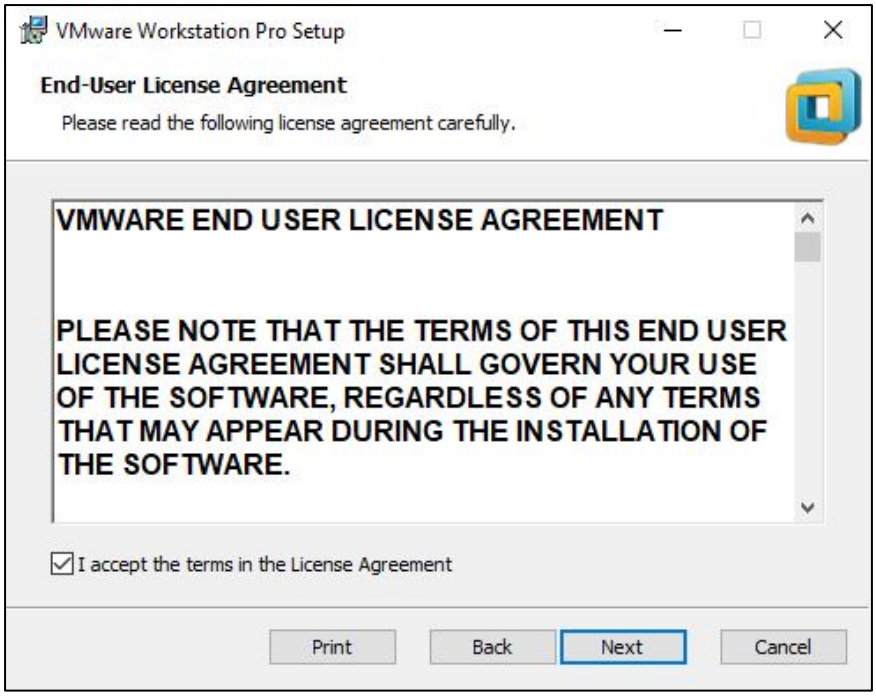


Figura E.3 Aceptación de acuerdos de licencia
Fuente: elaboración propia

Una vez hayan sido aceptados, se hace click sobre “Next”.

Paso 3:

En este paso se nos pide que indiquemos la ubicación de los archivos de instalación y el permiso para mejorar los driver del teclado.

La ubicación de los archivos se dejará la que está por defecto.

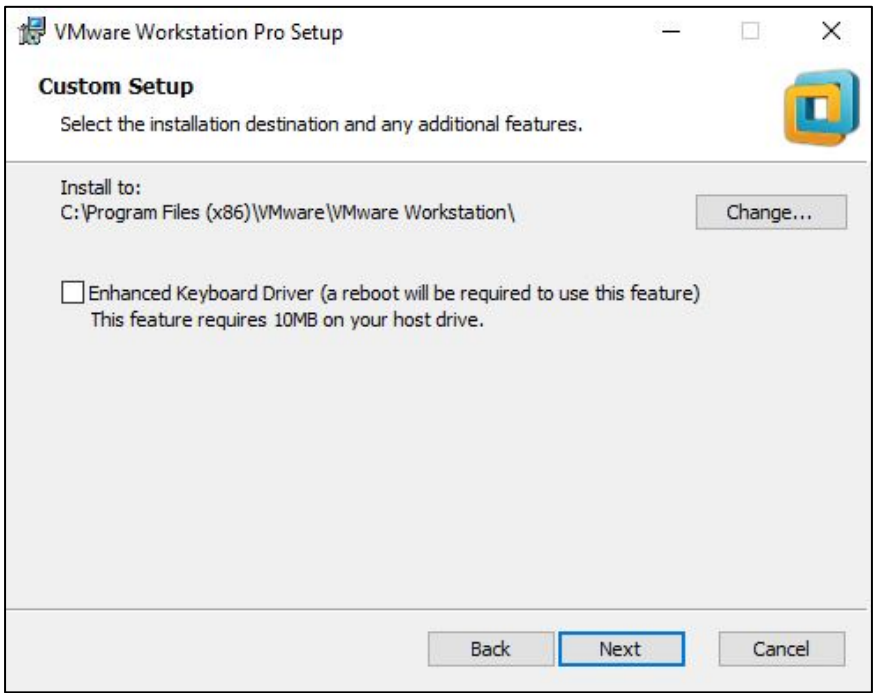


Figura E.4 Instalación driver de teclado
Fuente: elaboración propia

La mejora de los driver del teclado se instalará, haciendo click sobre la pestaña que se indica a continuación.

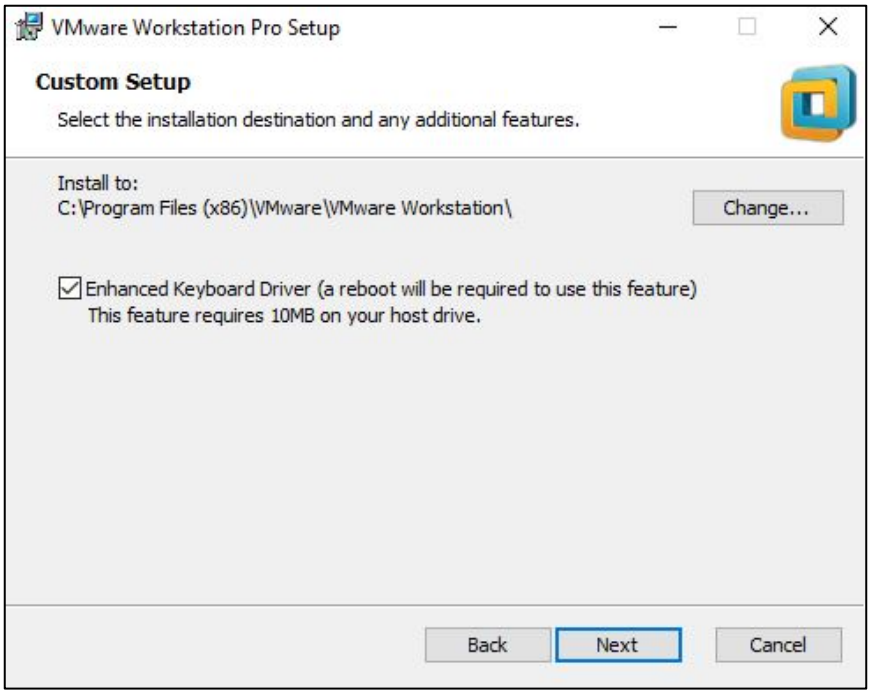


Figura E.5 Aceptación de instalación driver de teclado
Fuente: elaboración propia

Para continuar se hace click sobre “Next”.

Paso 4:

En este paso se solicita permiso para comprobar posibles actualizaciones del software e intercambiar informes con la empresa desarrolladora para la mejora del mismo. Dado que el sistema no dispondrá de conexión a internet, se dejan las dos pestañas sin seleccionar.

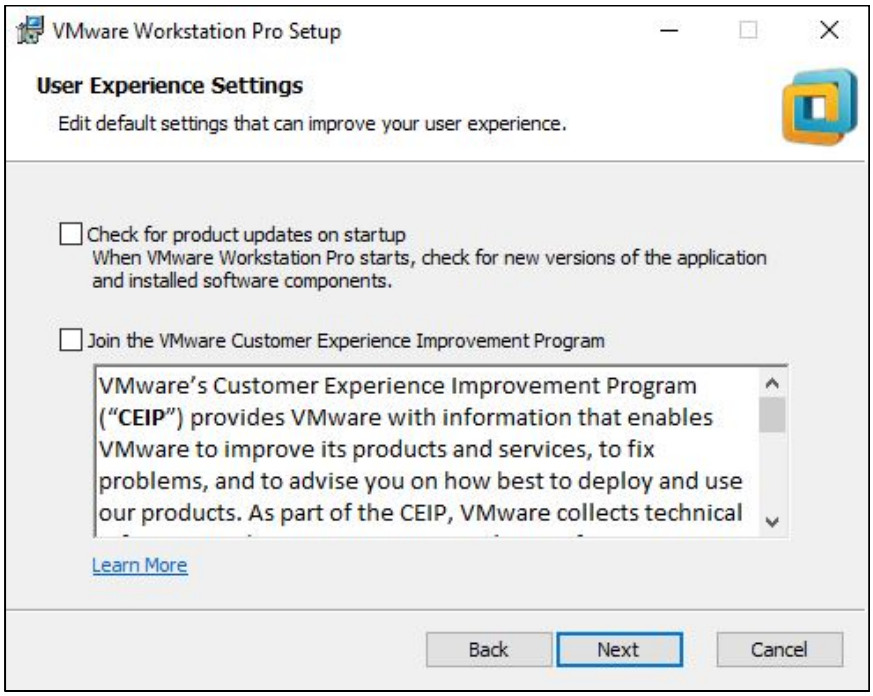


Figura E.6 Permisos para actualizaciones
Fuente: elaboración propia

Para continuar se hace click sobre "Next".

Paso 5:

En este paso se puede seleccionar los accesos directos del software que se crearán. Para facilitar el acceso al mismo se dejarán seleccionadas las dos pestañas, creando un acceso en el escritorio y otro en el menú de inicio del equipo.

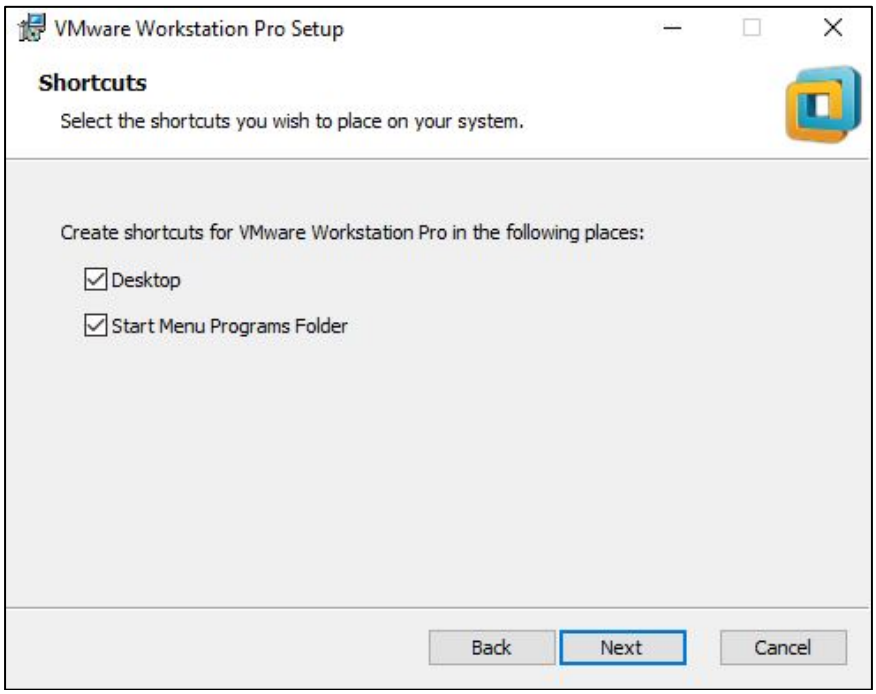


Figura E.7 Creación de accesos directos
Fuente: elaboración propia

Para continuar se hace click sobre “Next”.

Paso 6:

En este paso el instalador nos indica que esta todo listo para proceder a la instalación del software.

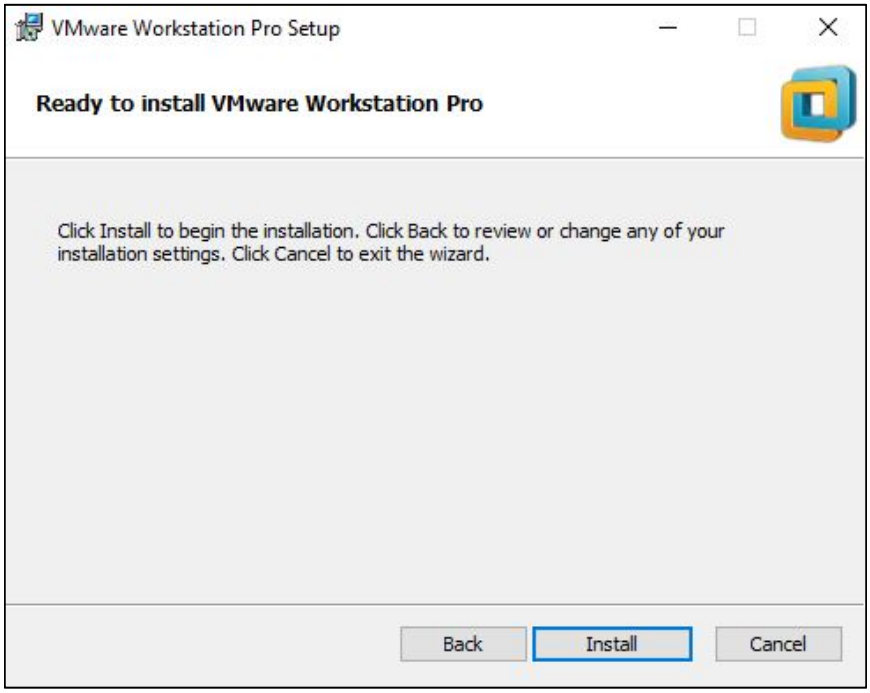


Figura E.8 Finalización de instalación
Fuente: elaboración propia

Para continuar se hace click sobre “Next”.

Paso 7:

En este paso el instalador nos indica el proceso de instalación. Llegados a este punto, el usuario solo tiene que esperar a que finalice la instalación.

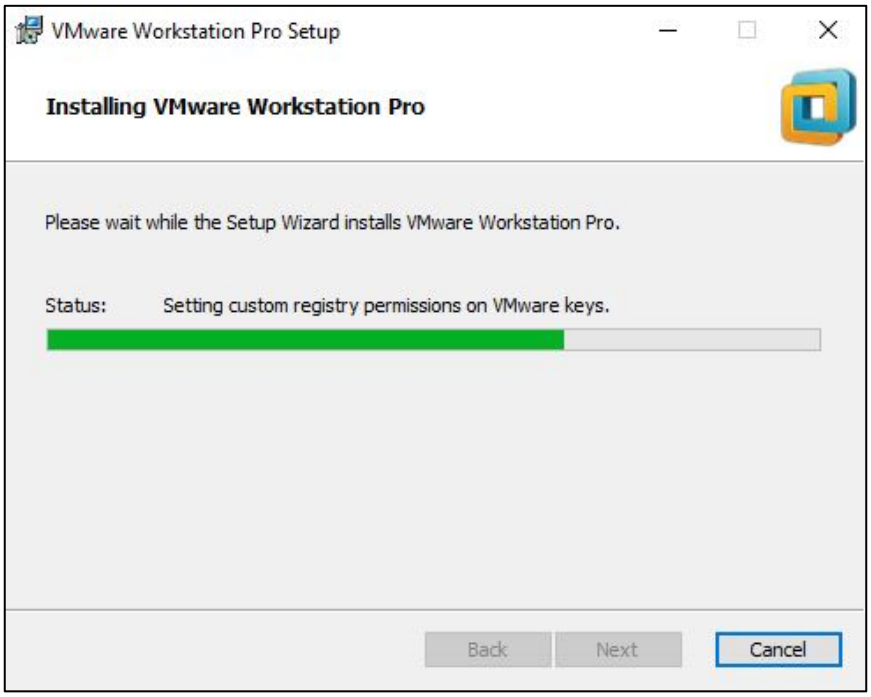


Figura E.9 Proceso de instalación
Fuente: elaboración propia

Una vez finalice el paso 7, el instalador pasa automáticamente al paso 8.

Paso 8:

En este paso el instalador nos indica que la instalación ha sido complementada con éxito.

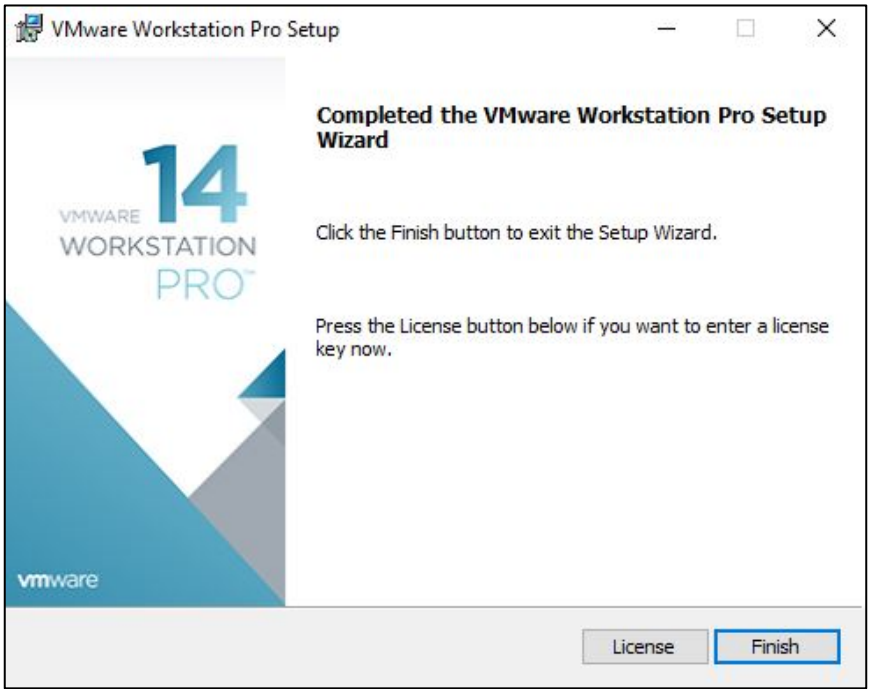


Figura E.10 Finalización y salida de asistente
Fuente: elaboración propia

Una vez haya finalizado la instalación con éxito se hace click sobre “Finish”.

Paso 9:

Tras haber finalizado el proceso de instalación, es necesario reiniciar el sistema para completar dicha instalación. Para ello, el instalador genera un aviso como el siguiente:

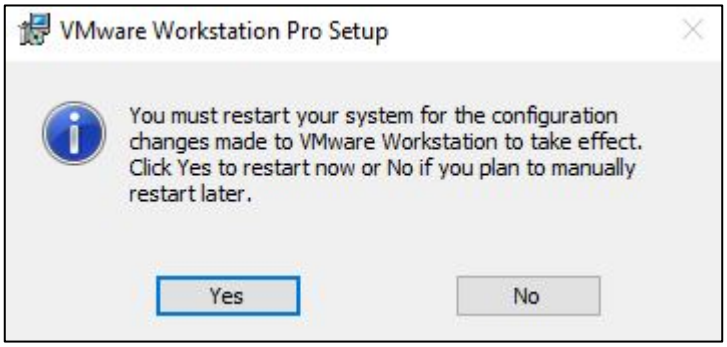


Figura E.11 Reinicio de equipo
Fuente: elaboración propia

Para finalizar el proceso se debe hacer click en “Yes” y esperar a que el sistema se reinicie.

Anexo F: Instalación de Windows Server 2012 R2

El Anexo F conforma la guía para la instalación del servidor Windows Server 2012 R2, máquina virtual que será la base para la instalación del resto de máquinas virtuales planteadas en la memoria.

Paso 1:

En este paso hay que pulsar sobre “Create a New Virtual Machine” para iniciar la creación de la VM e instalación del software necesario en esta:

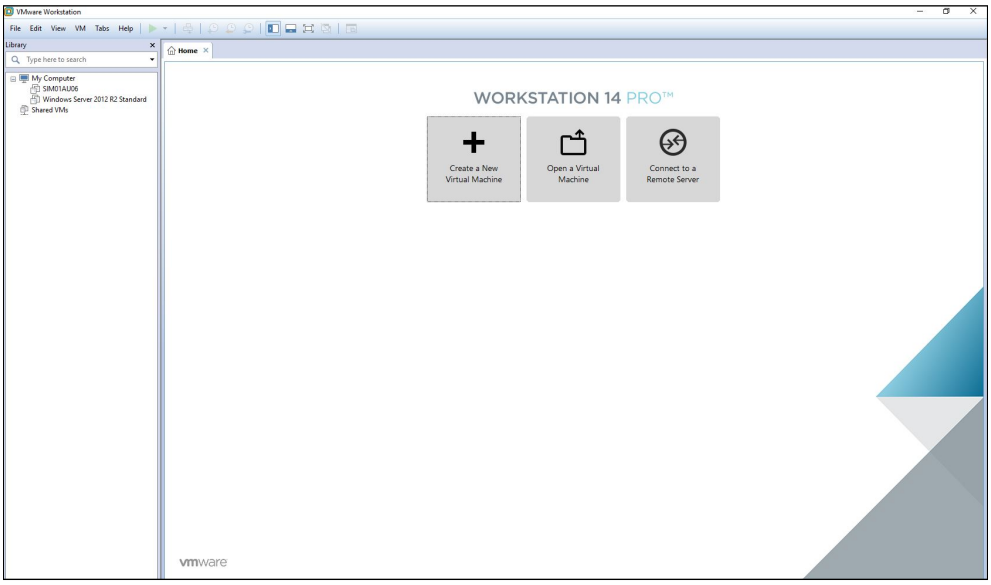


Figura F.1 Pantalla inicial de VMware
Fuente: elaboración propia

Paso 2:

El tipo de instalación que se va a elegir es Typical. Para ello, se elige este tipo y se hace click sobre “Next” para continuar:

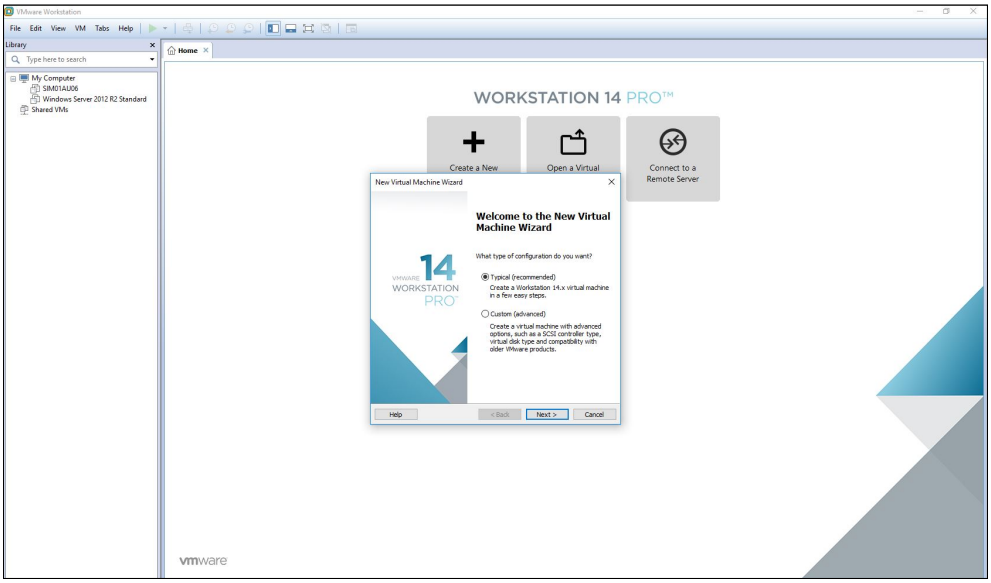


Figura F.2 Inicio de creación de máquina virtual
Fuente: elaboración propia

Paso 3:

En este paso se selecciona la imagen de disco que se va a utilizar para la instalación de Windows Server en la máquina virtual:

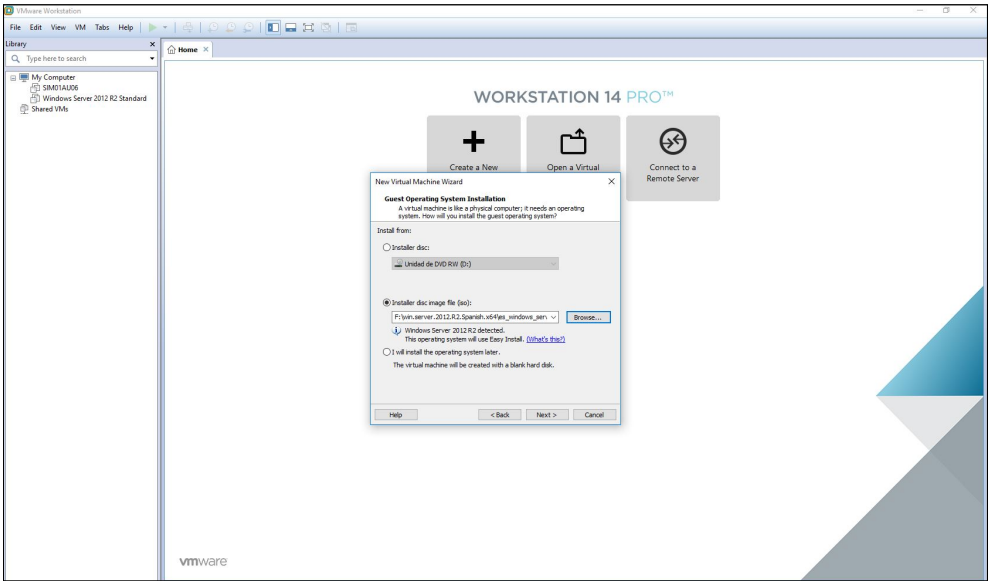


Figura F.3 Selección de imagen de disco para máquina virtual
Fuente: elaboración propia

Una vez se ha seleccionado, se hace click en “Next”.

Paso 4:

En este paso se realizan tres acciones: en primer lugar, escribir la clave del producto de Windows; en segundo lugar, el nombre que se desea dar al usuario principal del equipo; y en tercer lugar, la contraseña que desea establecer para acceder al equipo:

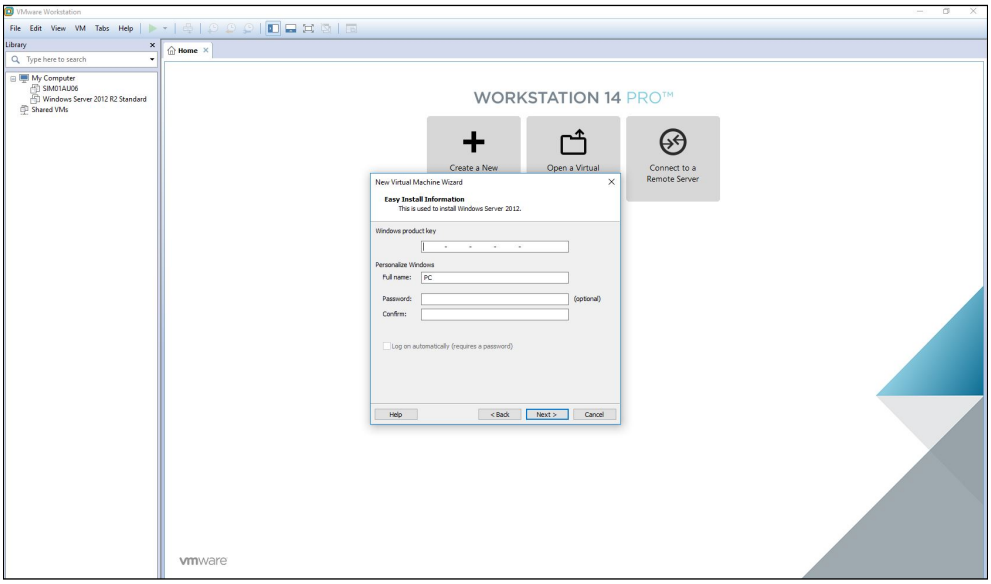


Figura F.4 Introducción de datos
Fuente: elaboración propia

Para continuar se hace click en “Next”.

Paso 5:

En este paso se selecciona el nombre que se desea dar a la máquina virtual y la ubicación de los archivos que la forman. Ambos se dejan por defecto:

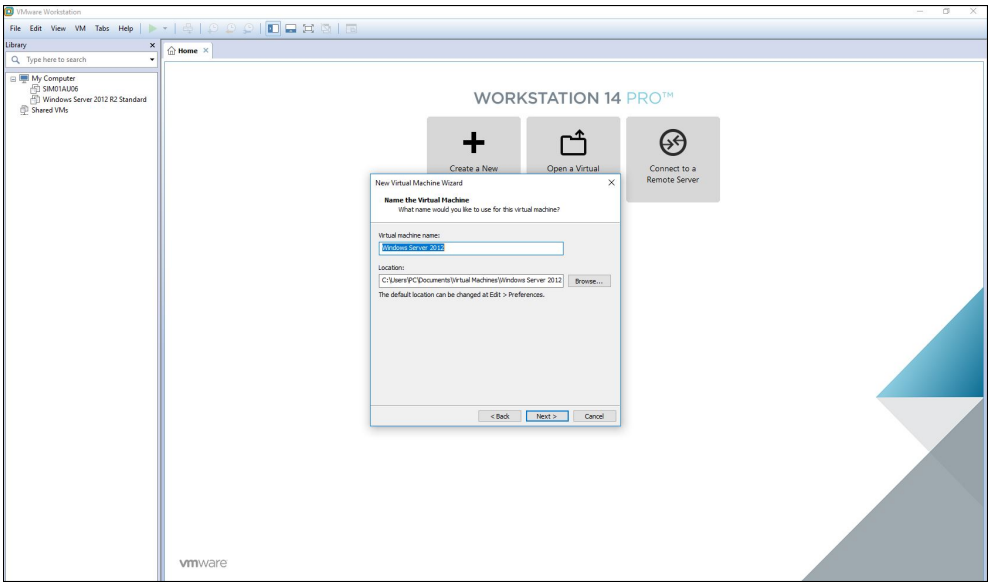


Figura F.5 Selección de nombre de la máquina virtual
Fuente: elaboración propia

Para seguir con la instalación se hace click sobre “Next”.

Paso 6:

En este paso se debe seleccionar si se desea que los archivos que forman el disco duro de la máquina virtual sean varios o uno fusionando a los demás. Esta configuración permite que en caso de que se tenga que copiar y pegar la maquina virtual en otro equipo, la operación sea mas rápida y sencilla (con la opción “Split virtual disk into multiple files”). En este caso, seleccionamos la opción de un disco duro:

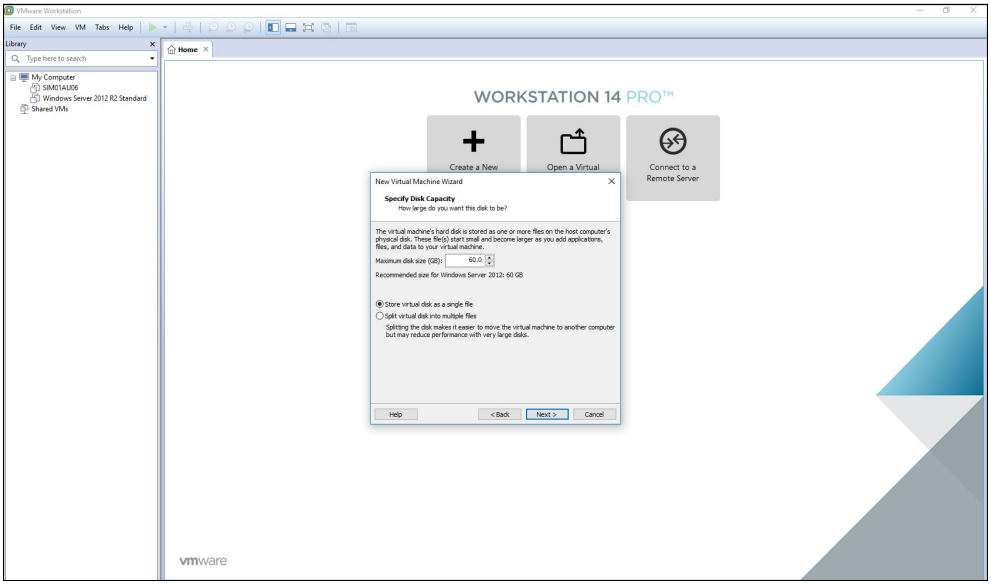


Figura F.6 Selección de tipo de disco duro
Fuente: elaboración propia

Para continuar se hace click sobre “Next”.

Paso 7:

En este paso se comprueba que las configuraciones establecidas en el proceso de instalación son correctas:

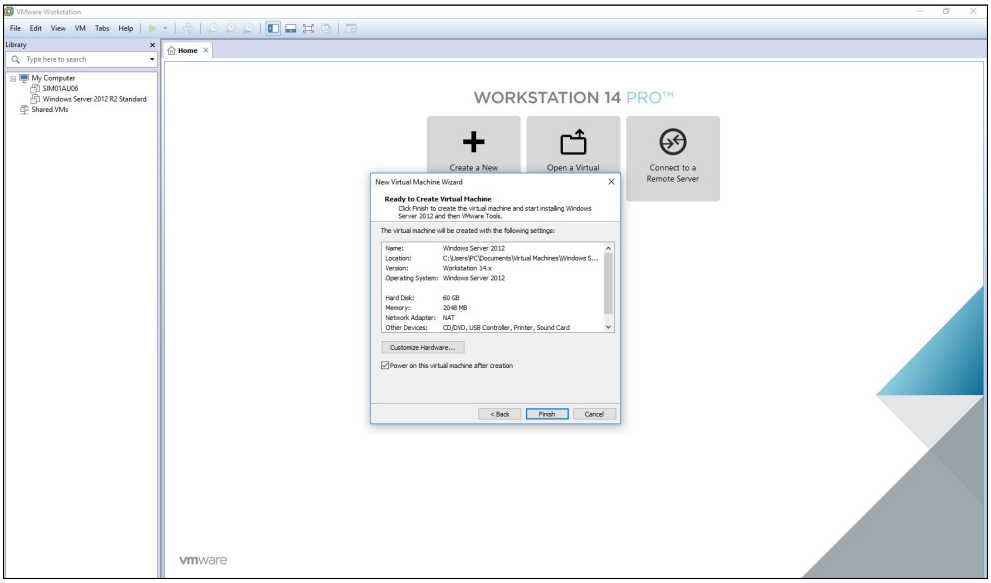


Figura F.7 Comprobación de configuraciones
Fuente: elaboración propia

Una vez se han realizado las comprobaciones se hace click sobre “Finish”, para así dar inicio a la instalación.

Paso 8:

En este paso da comienzo el asistente de instalación de Windows Server:

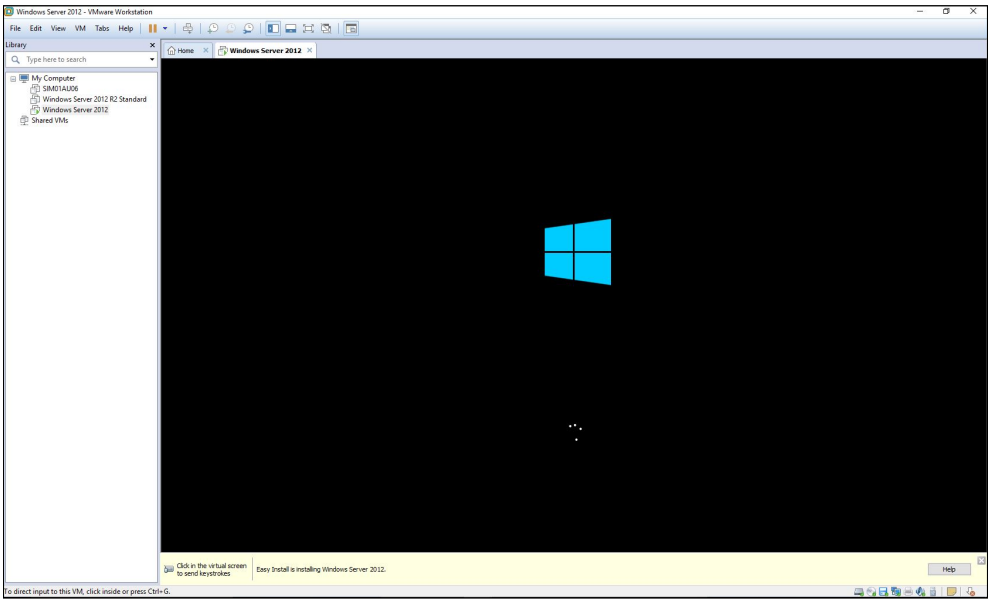


Figura F.8 Inicio de asistente de instalación de Windows Server
Fuente: elaboración propia

Llegados a este punto, se debe seleccionar el Sistema operativo “Windows Server 2012 R2 Standard (instalación Server Core)”:

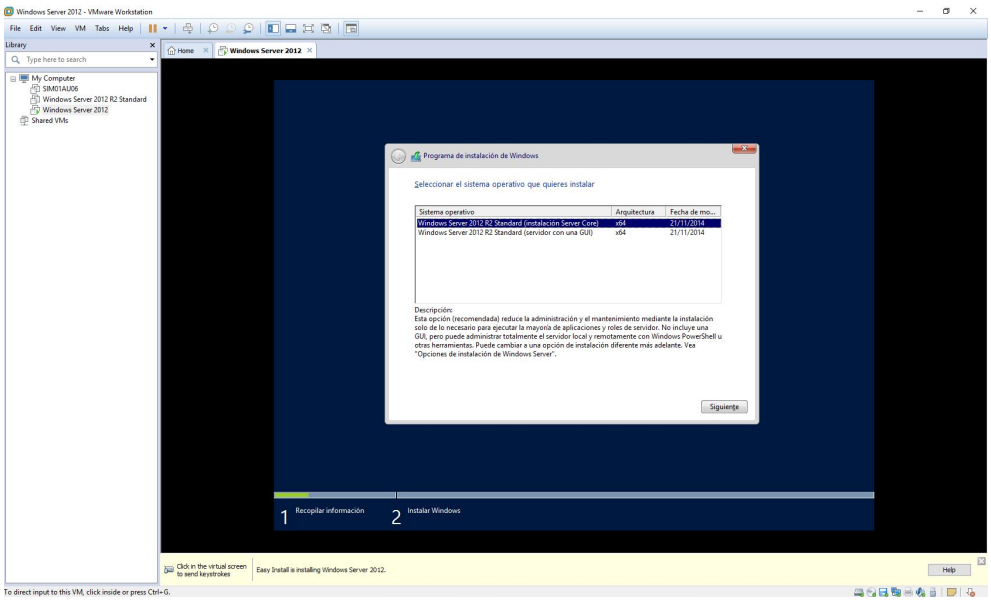


Figura F.9 Selección de versión de Windows Server
Fuente: elaboración propia

A continuación se hace click sobre “Siguiente”.

Paso 9:

Tras seleccionar el Sistema operativo a instalar, da comienzo la instalación:

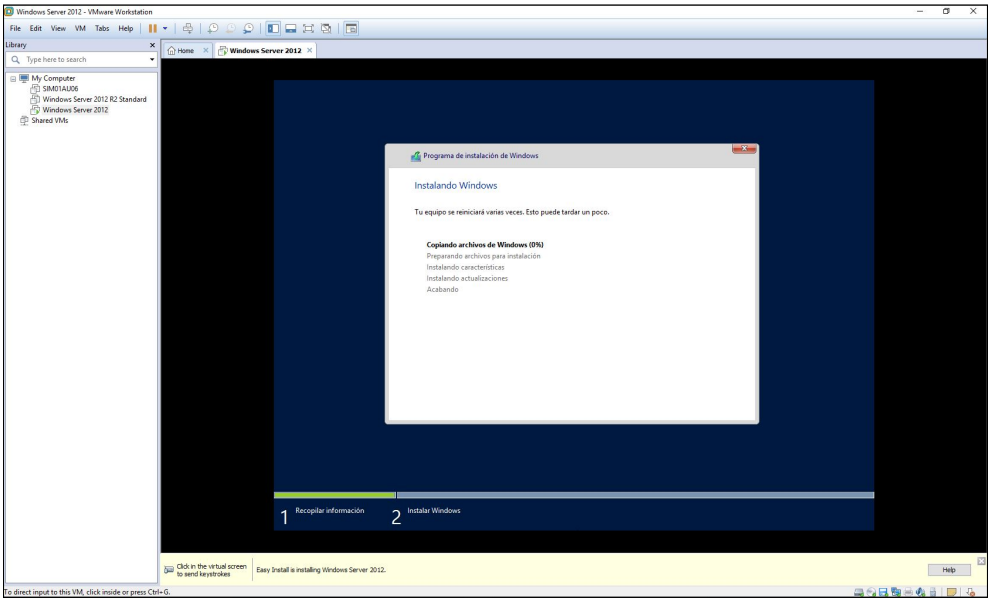


Figura F.10 Proceso de instalación
Fuente: elaboración propia

Una vez la instalación ha sido realizada, el asistente solicita reiniciar el equipo para que los cambios realizados surtan efecto:

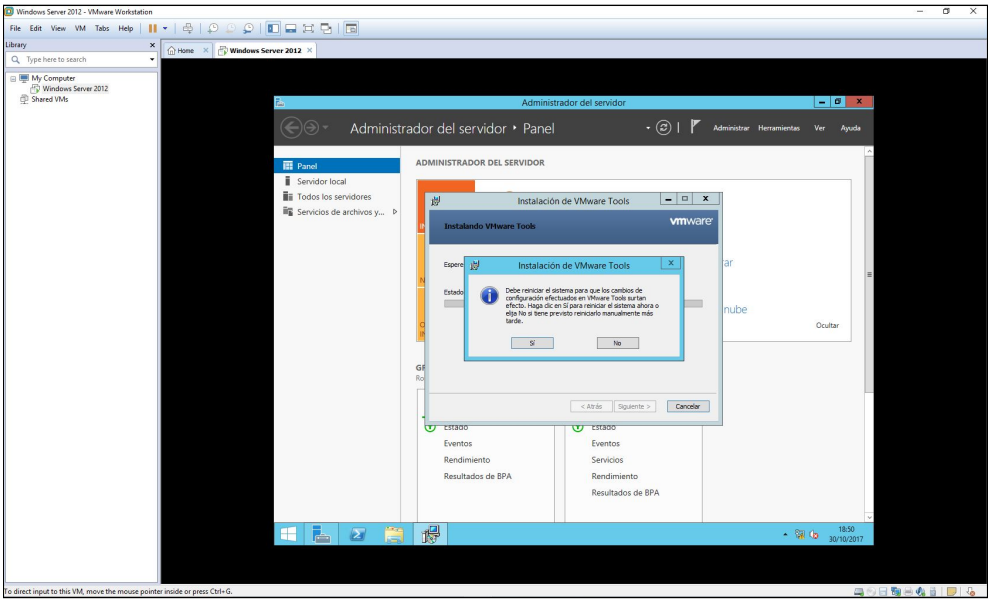


Figura F.11 Finalización de instalación y reinicio de equipo
Fuente: elaboración propia

Tras el reinicio, el equipo nos muestra la pantalla inicial del Administrador del Servidor, dando por finalizada la instalación:

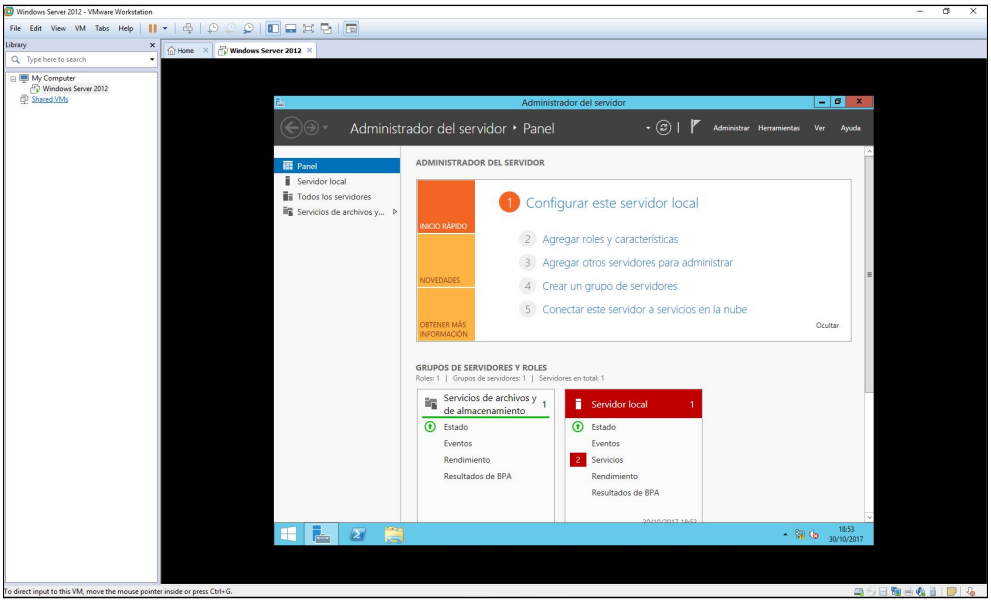


Figura F.12 Pantalla inicial del Administrador del Servidor
Fuente: elaboración propia

Anexo G: Instalación de Active Directory Domain Server

El Anexo G muestra la agregación de roles y características de Active Directory y el proceso para promover el servidor a controlador de dominio, creando así una de las máquinas virtuales establecidas en el punto 4.2 “Creación de máquinas virtuales en VMware” de la memoria.

En primer lugar es necesario configurar el direccionamiento IP manualmente y cambiar el nombre del equipo, explicado en los pasos iniciales de este anexo.

Paso 1:

En este paso se configura el direccionamiento IP de la red creada, en este caso el direccionamiento a utilizar es el mostrado en las siguientes capturas de pantalla. Este paso no es parte como tal de la instalación de Active Directory, pero son una serie de configuraciones iniciales necesarias.

Para ello, nos dirigimos a las Conexiones de Red del equipo:

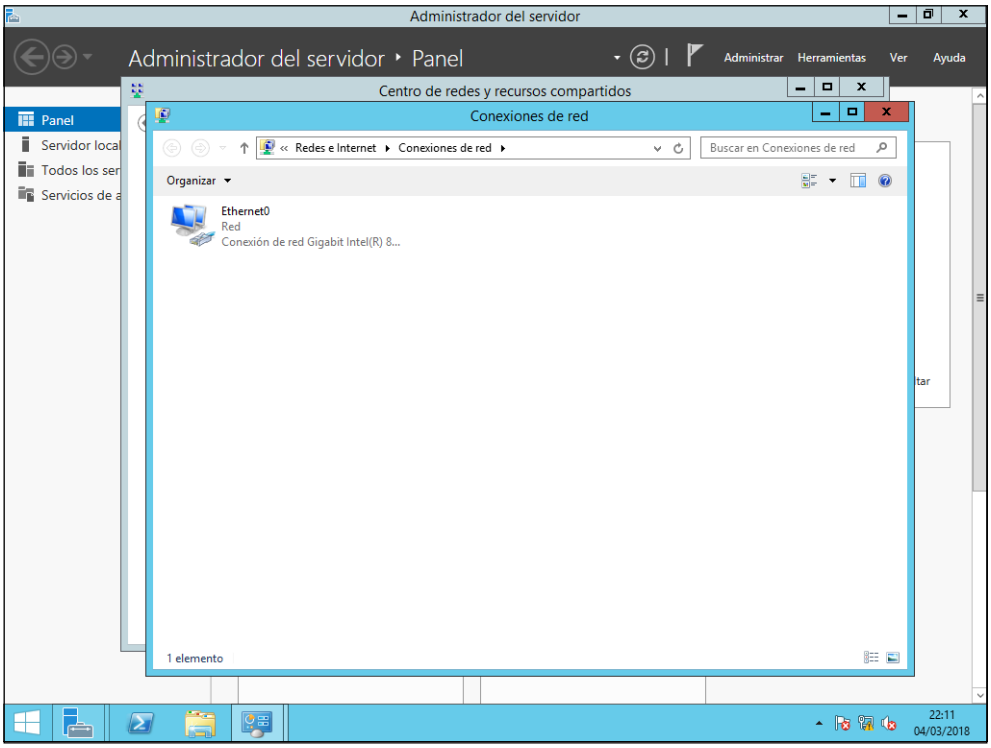


Figura G.1 Conexiones de Red del equipo
Fuente: elaboración propia

Se accede a las propiedades de la conexión. En Protocolo de Internet versión 4 (TCP/IPv4) se cambia el direccionamiento IP y se hace click en “Aceptar”.

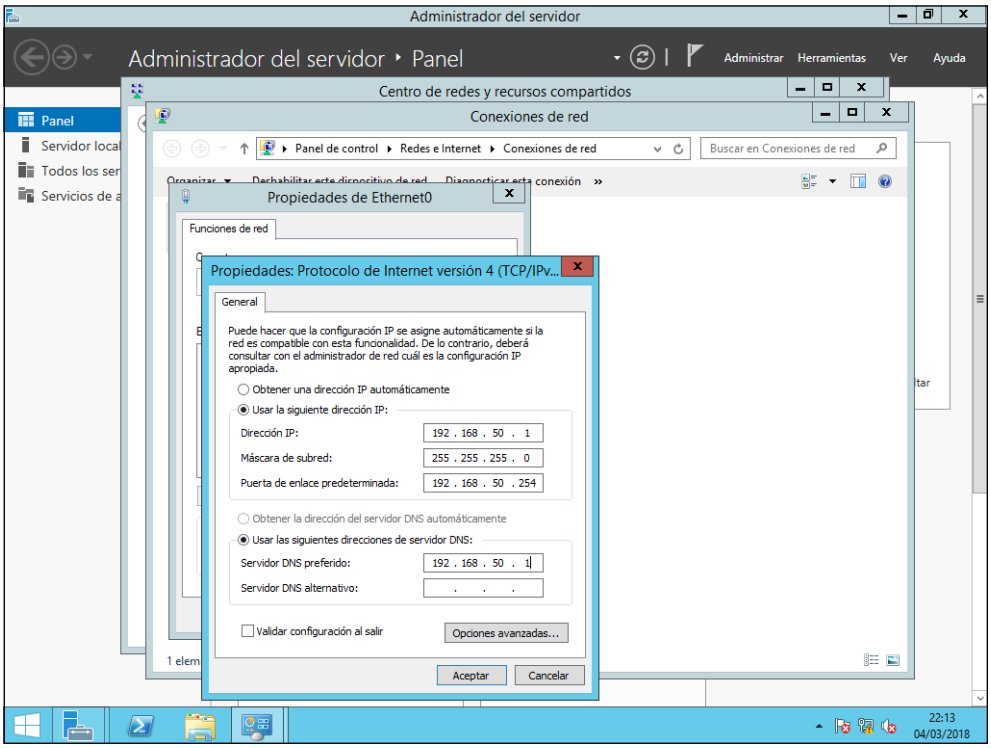


Figura G.2 Configuración protocolo IPv4
Fuente: elaboración propia

Tras configurar el direccionamiento IP, nos dirigimos a Administrador del Servidor/ Servidor Local para cambiar el nombre de equipo. Se pulsa en “Nombre de equipo”:

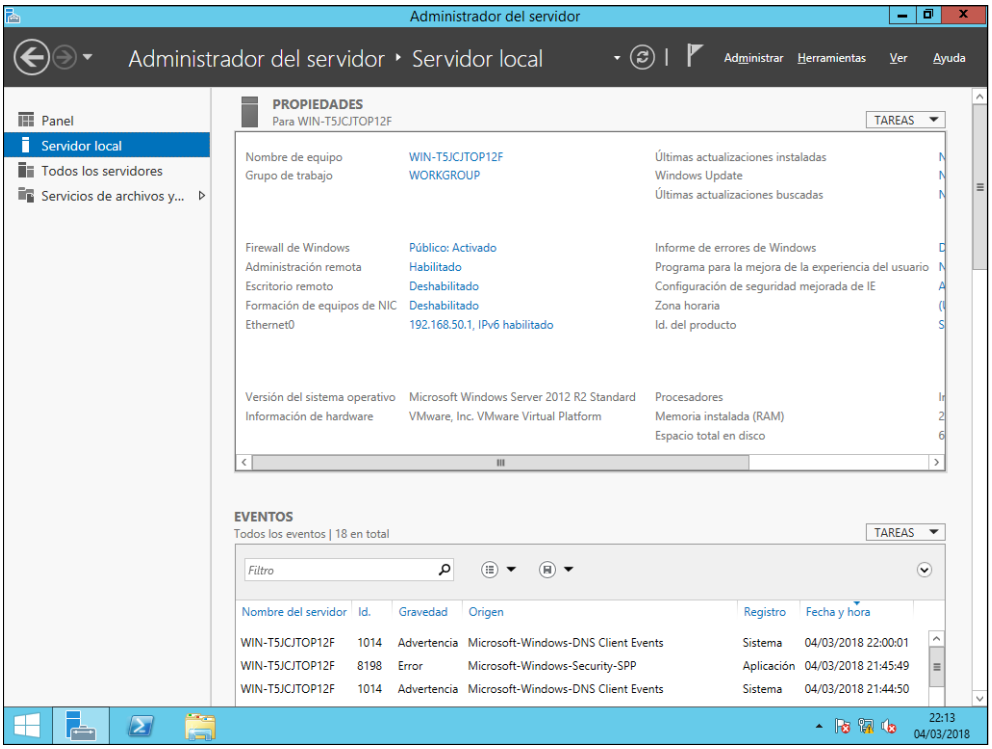


Figura G.3 Cambio del nombre de equipo
Fuente: elaboración propia

Se pone como nombre de equipo “Administrador” y se hace click en “Aceptar”.

A continuación se solicita permiso para reiniciar el equipo y aplicar los cambios realizados. Se pulsa en “Reiniciar ahora”:

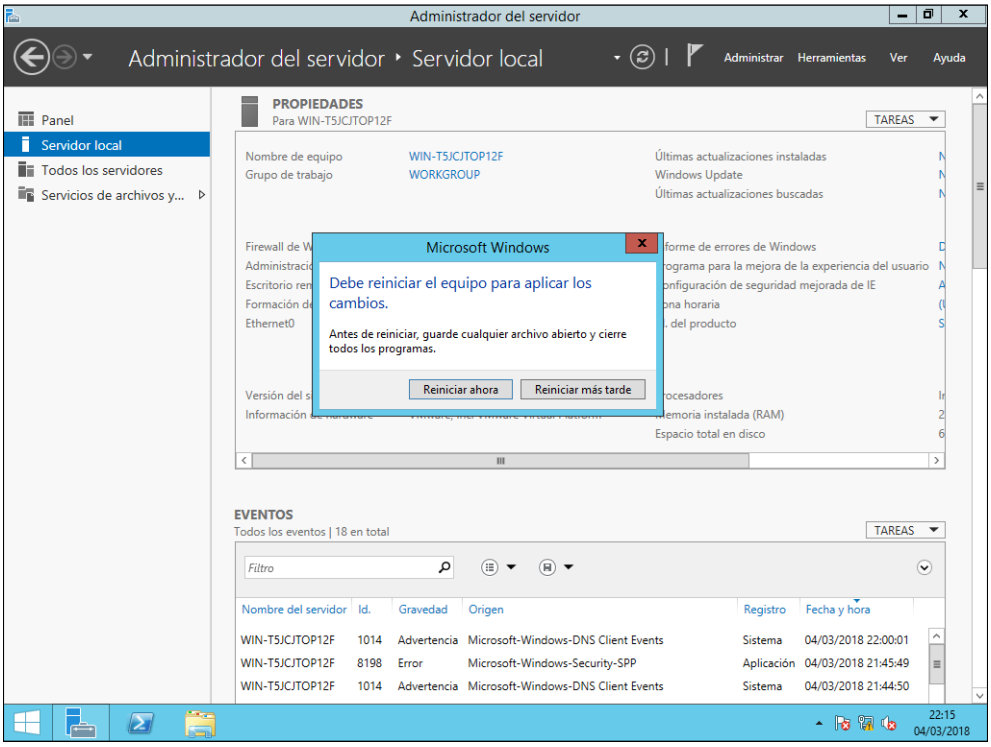


Figura G.4 Reinicio de equipo
Fuente: elaboración propia

Tras el reinicio, se accede al equipo con la contraseña establecida en la creación de la máquina virtual:

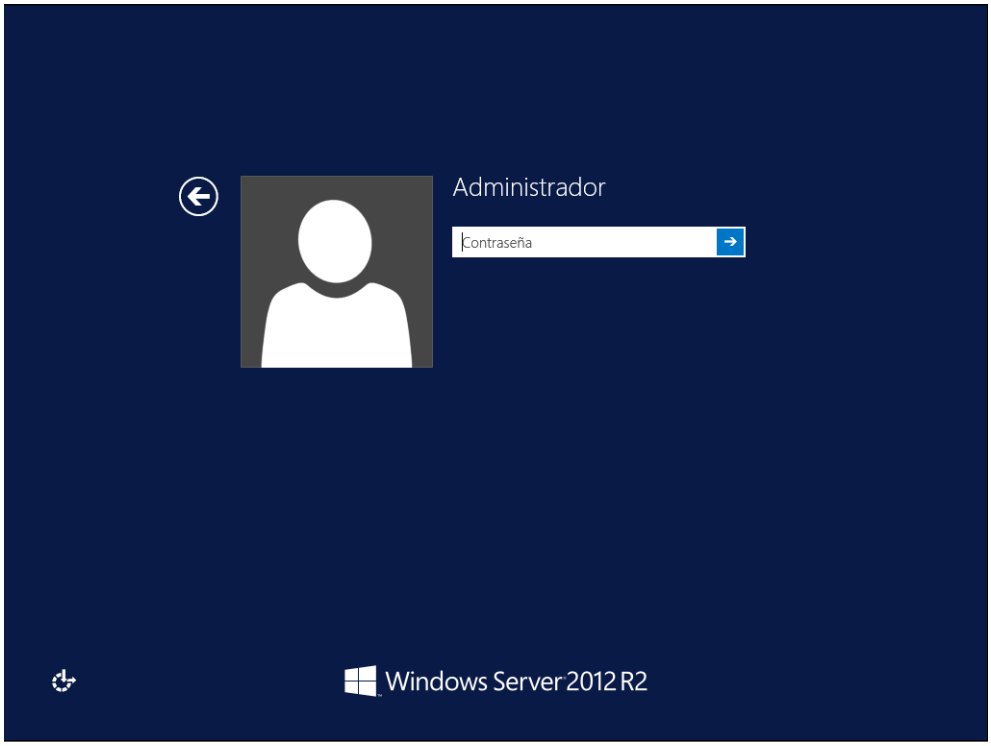


Figura G.5 Acceso al equipo
Fuente: elaboración propia

Paso 2:

Tras las configuraciones previas iniciales, se inicia la instalación de Active Directory Domain Server. Para ello, se hace click en el punto 2 " Agregar roles y características":

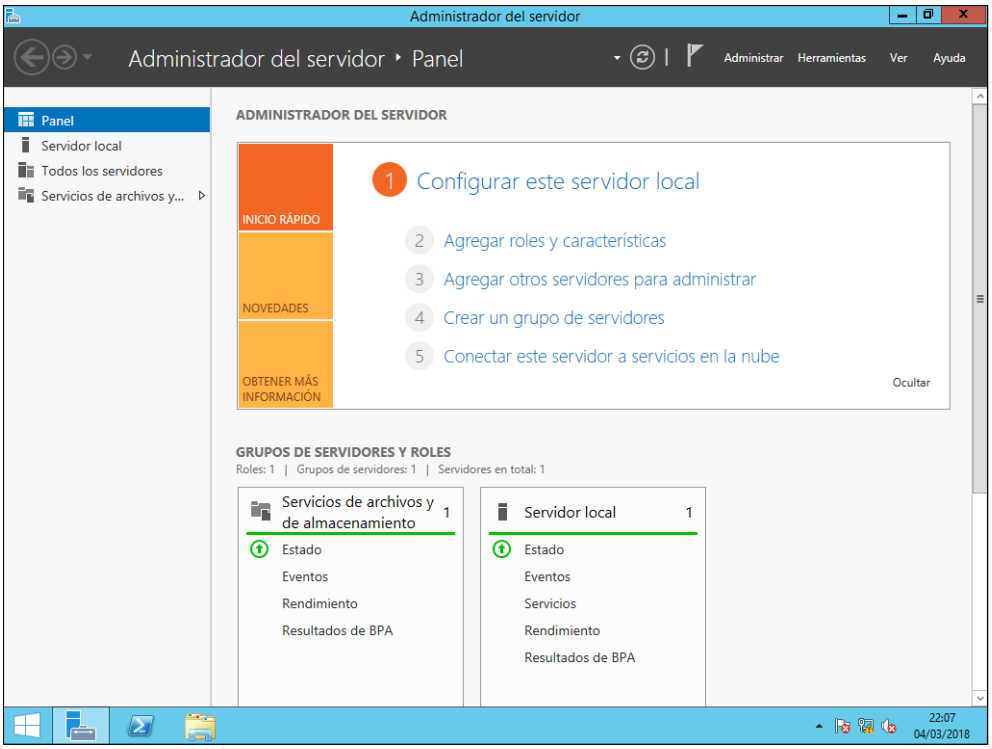


Figura G.6 Inicio asistente de instalación de AD DS
Fuente: elaboración propia

En el primer paso, no se tiene que realizar ninguna configuración. Se hace click en “Siguiente”:

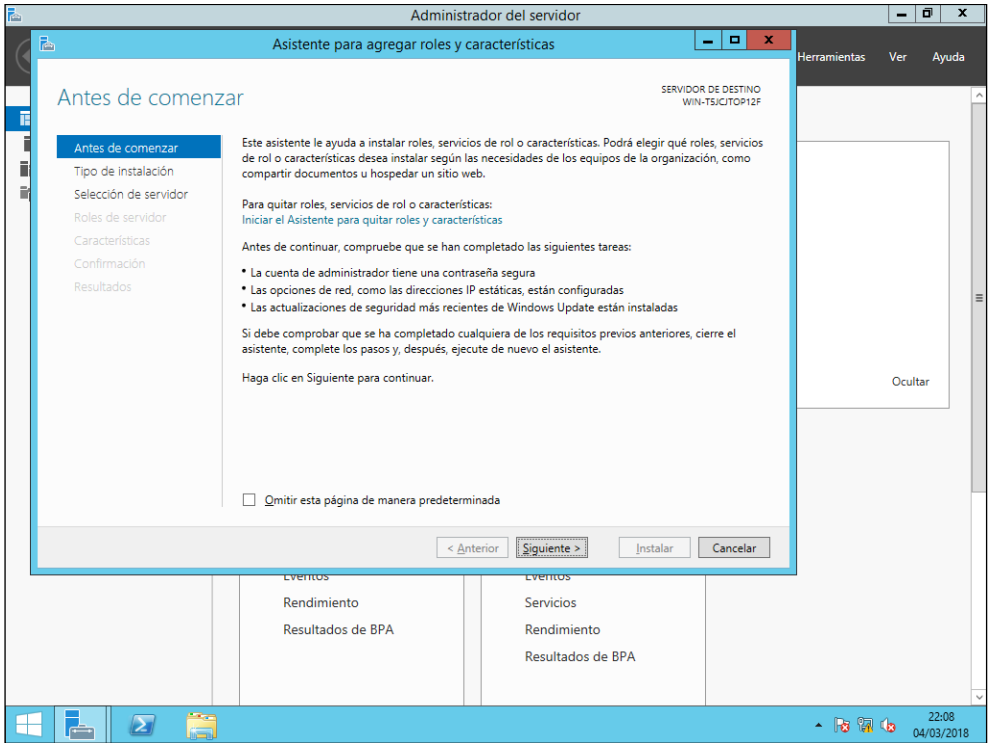


Figura G.7 Primer paso de instalación de AD DS
Fuente: elaboración propia

Paso 3:

En este paso se selecciona “Instalación basada en características o en roles” y se hace click en “Siguiente”:

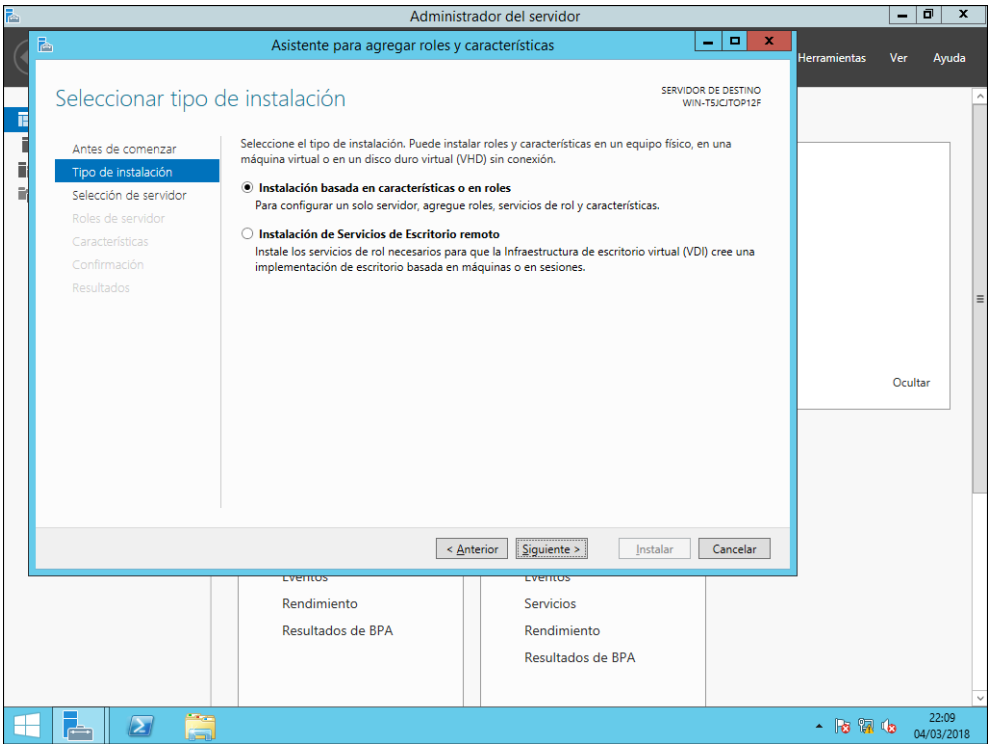


Figura G.8 Selección de tipo de instalación
Fuente: elaboración propia

Paso 4:

En este paso se selecciona el servidor sobre el que se quiere instalar el rol de Active Directory. Para ello, se selecciona el servidor que se ha creado anteriormente con el nombre y direccionamiento IP indicados:

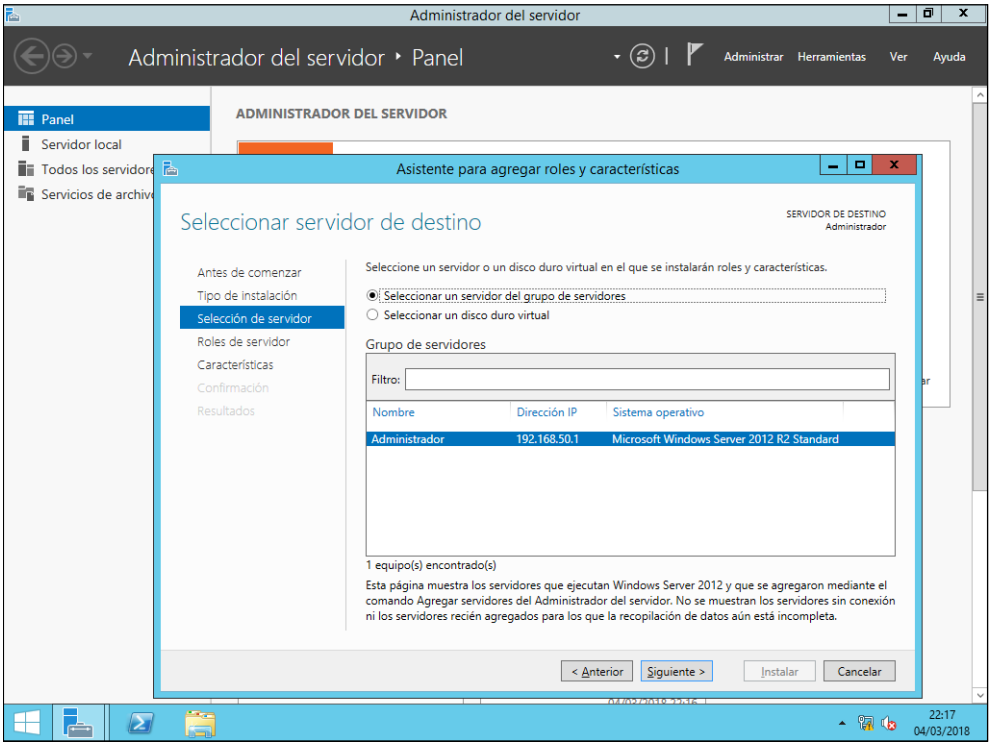


Figura G.9 Selección de servidor
Fuente: elaboración propia

Tras elegir el servidor se hace click en “Siguiente”.

Paso 5:

En este paso se eligen los roles que se desean instalar en el servidor. En este caso, se selecciona el rol de “Servicios de dominio de Active Directory”. Tras elegir el rol se hace click en “Siguiente”:

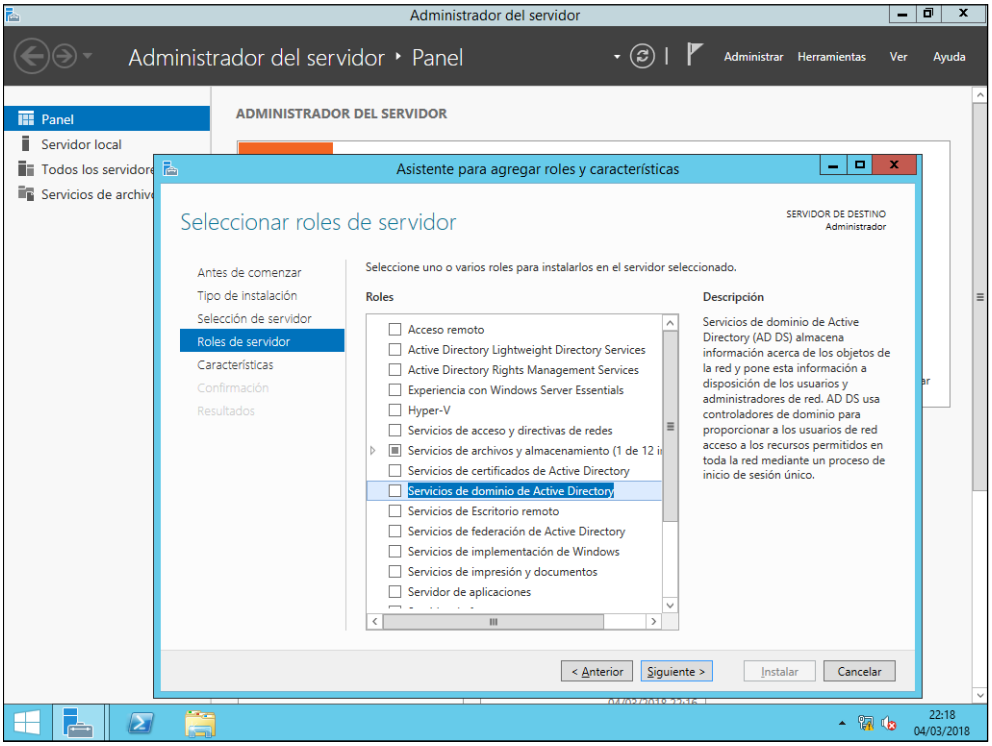


Figura G.10 Selección de roles
Fuente: elaboración propia

A continuación el asistente pide que se dé permiso para agregar las características requeridas por Active Directory. Para ello, se hace click en “Agregar características”:

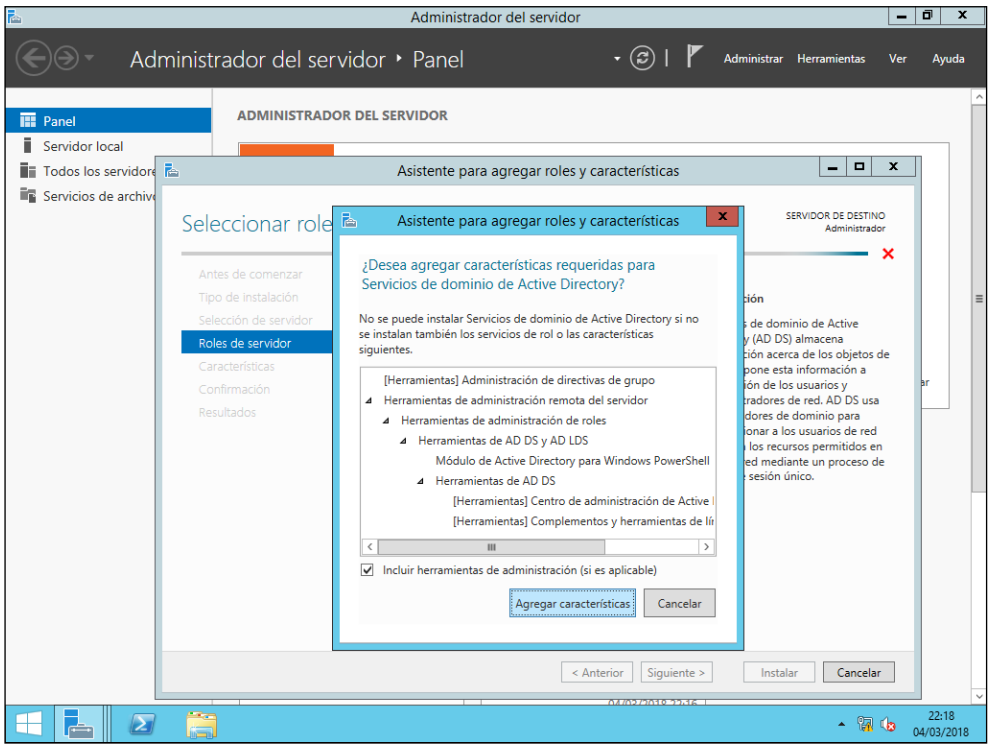


Figura G.11 Permiso para agregar características
Fuente: elaboración propia

Paso 6:

En este paso se eligen las características que se desean instalar. Se comprueba que "Administración de directivas de grupo" está seleccionado:

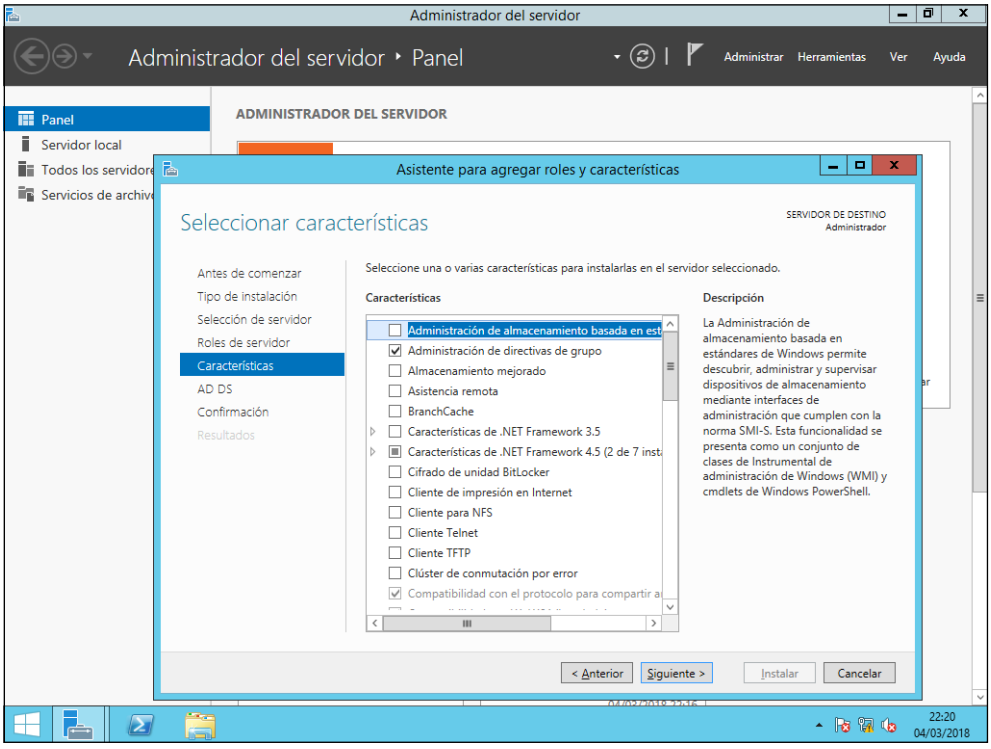


Figura G.12 Selección de características
Fuente: elaboración propia

Tras la comprobación, se hace click en "Siguiente".

Paso 7:

En este paso se muestran explicaciones sobre los elementos que se van a instalar en el servidor.

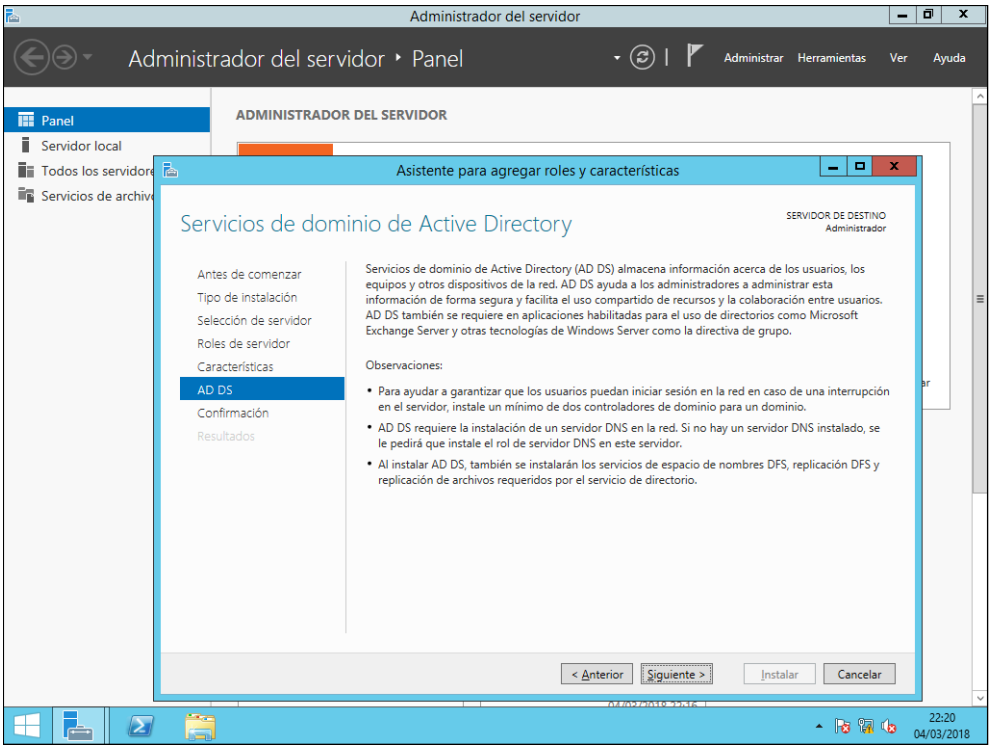


Figura G.13 Explicaciones sobre elementos a instalar
Fuente: elaboración propia

Tras haberlas leído se hace click en “Siguiente”.

Paso 8:

En este paso se muestran los elementos que se van a instalar.

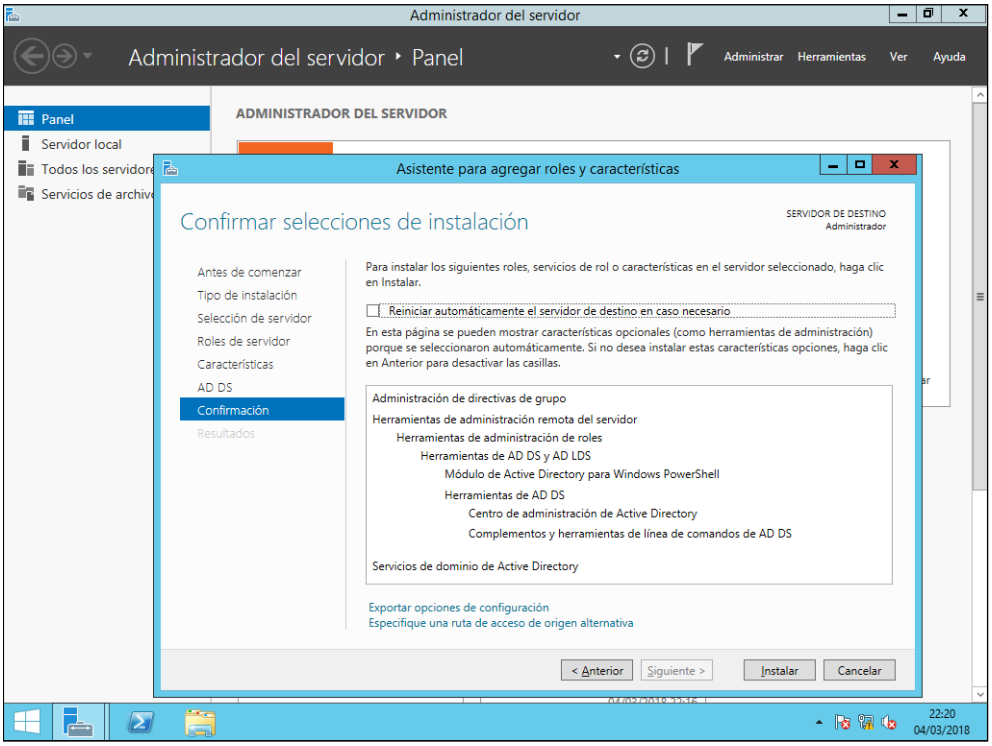


Figura G.14 Visualización de elementos a instalar
Fuente: elaboración propia

Tras haber comprobado los elementos a instalar se hace click en “Instalar”.

Paso 9:

En este paso se inicia la instalación de Active Directory, mostrado en la siguiente captura de pantalla:

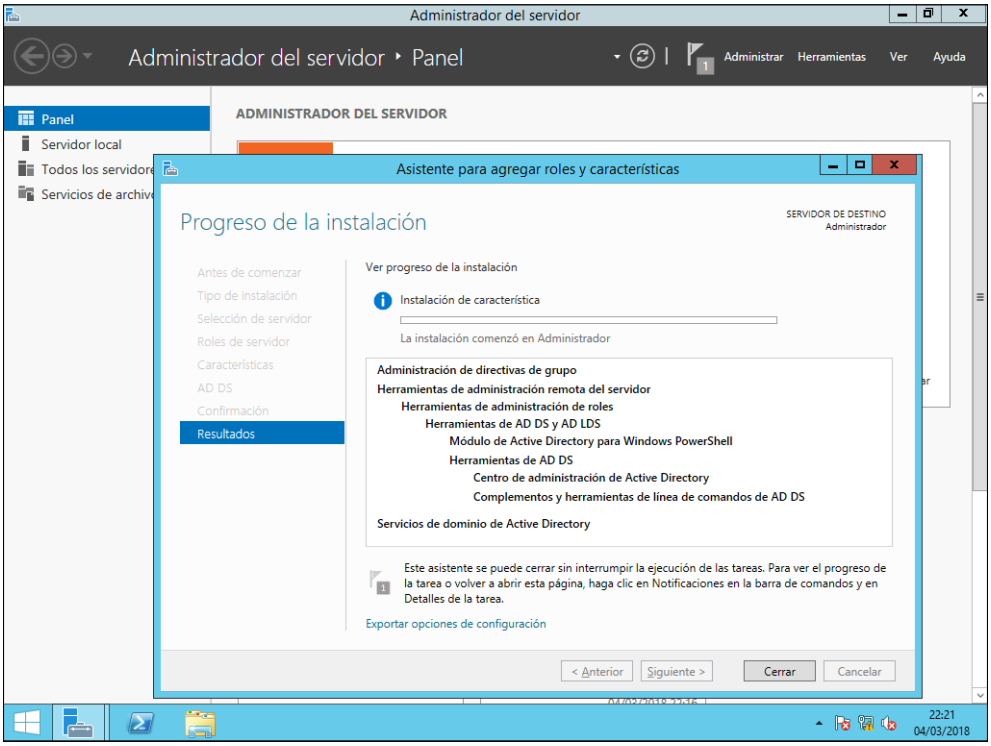


Figura G.15 Inicio de proceso de instalación
Fuente: elaboración propia

Tras finalizar, la barra de progreso queda completa, mostrando los elementos instalados:

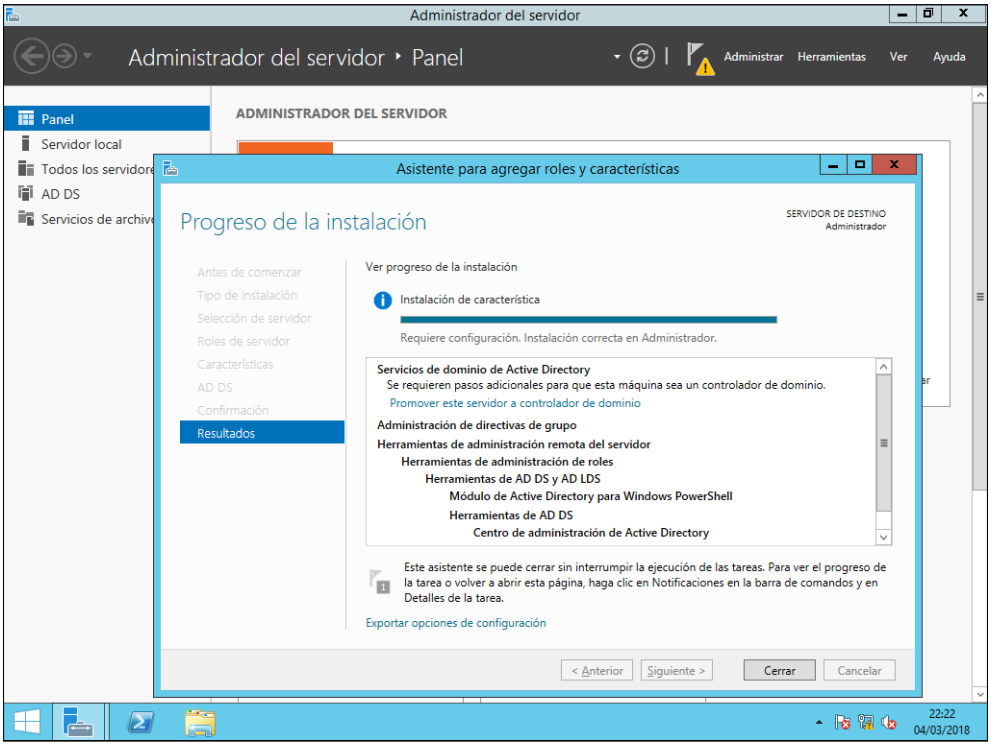


Figura G.16 Finalización de instalación de AD DS
Fuente: elaboración propia

Para finalizar se hace click en “Cerrar”.

Paso 10:

En este paso se inicia el proceso para promover el servidor a controlador de dominio. Para ello, se debe cerrar sesión e iniciar el equipo como el usuario “Administrator” que el servidor crea por defecto.

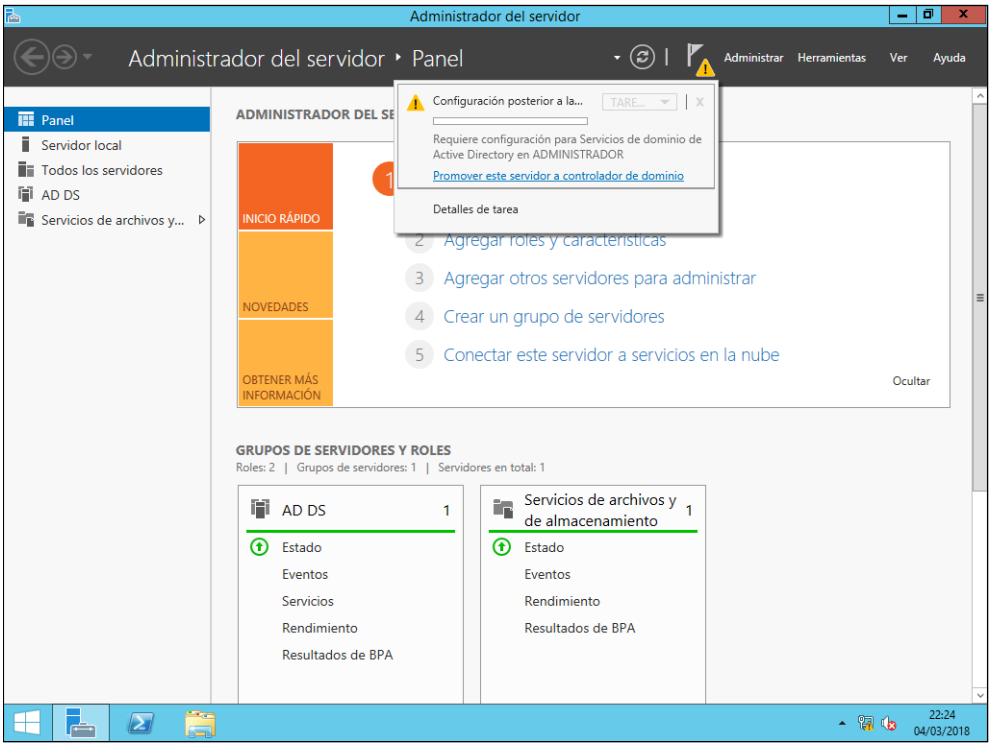


Figura G.17 Inicio de promover servidor a controlador de dominio
Fuente: elaboración propia

A continuación se hace click sobre “Promover este servidor a controlador de dominio”, iniciando así el asistente de configuración de Active Directory.

Paso 11:

En este paso se inicia el proceso para promover el servidor a controlador de dominio. El primer paso es crear un nuevo bosque para el dominio que se utilizará en la red. Para ello, se selecciona la opción “Agregar un nuevo bosque” y se da nombre al dominio raíz, en este caso “SIMACET.local”

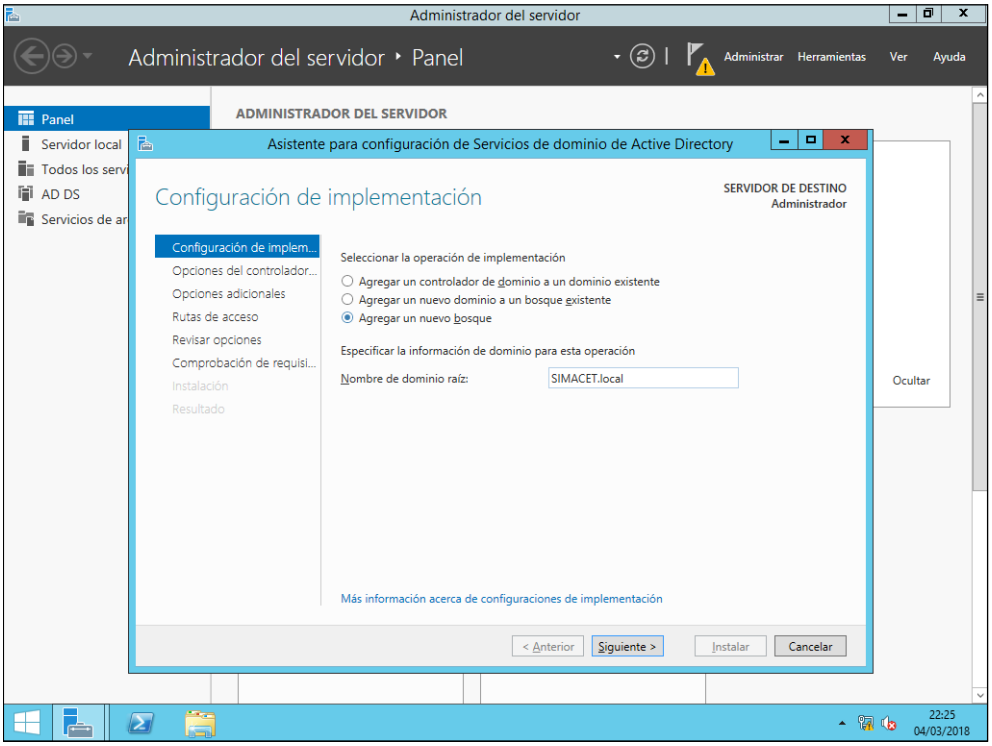


Figura G.18 Creación de nuevo bosque
Fuente: elaboración propia

A continuación se hace click sobre “Siguiente”.

Paso 12:

En este paso se pide seleccionar el nivel funcional del bosque y del dominio, que se deja el elegido por defecto (Windows Server 2012 R2). Además, hay que establecer la contraseña de modo de restauración de servicios de directorio (DSRM), necesaria para continuar con el asistente:

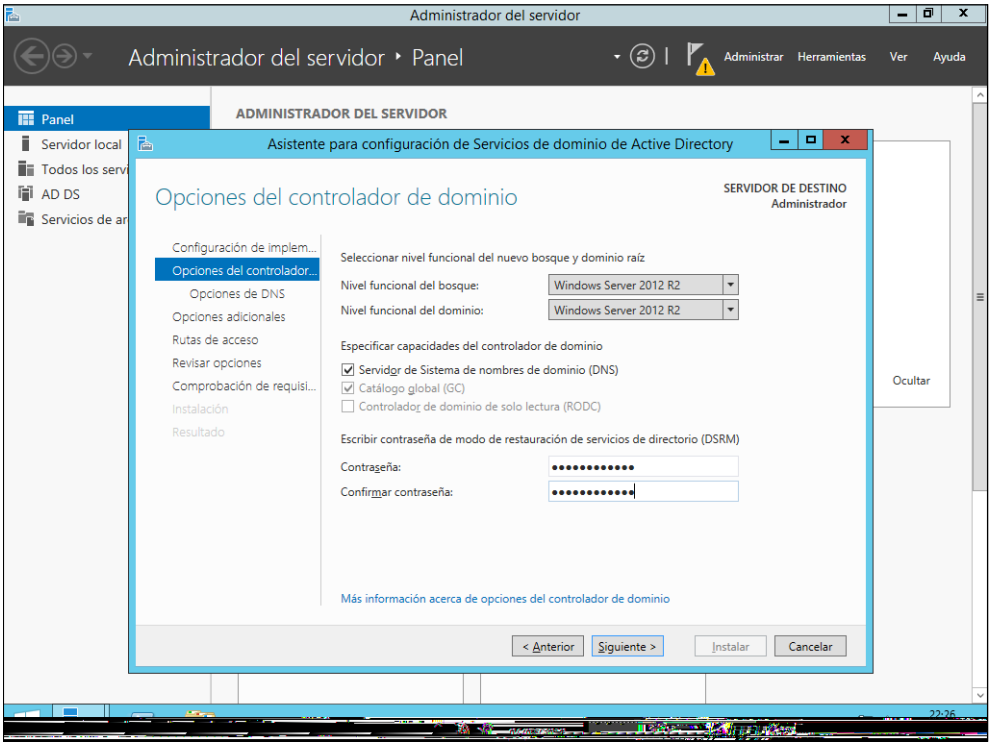


Figura G.19 Configuraciones del dominio
Fuente: elaboración propia

A continuación se hace click sobre “Siguiente”.

Paso 13:

En este paso no se hace nada, puesto que la configuración de DNS no se realiza en este asistente.

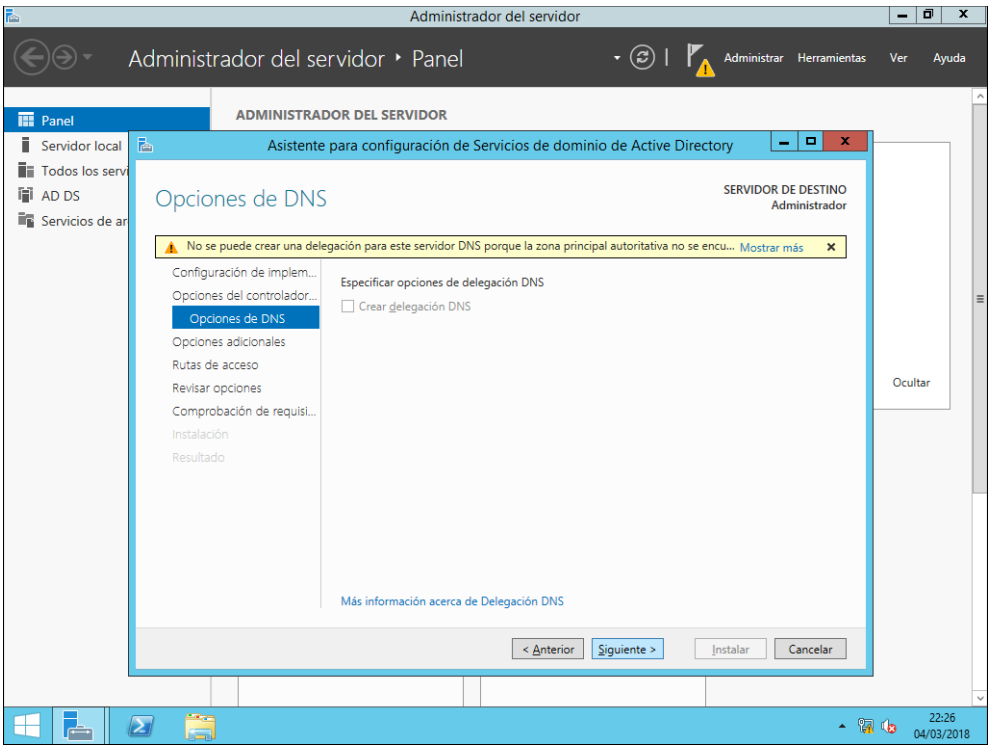


Figura G.20 Configuración de DNS
Fuente: elaboración propia

Para continuar se hace click sobre “Siguiente”.

Paso 14:

En este paso se da nombre al dominio NetBIOS, que por defecto se da el mismo que se ha dado al dominio raíz. Se deja el creado por defecto.

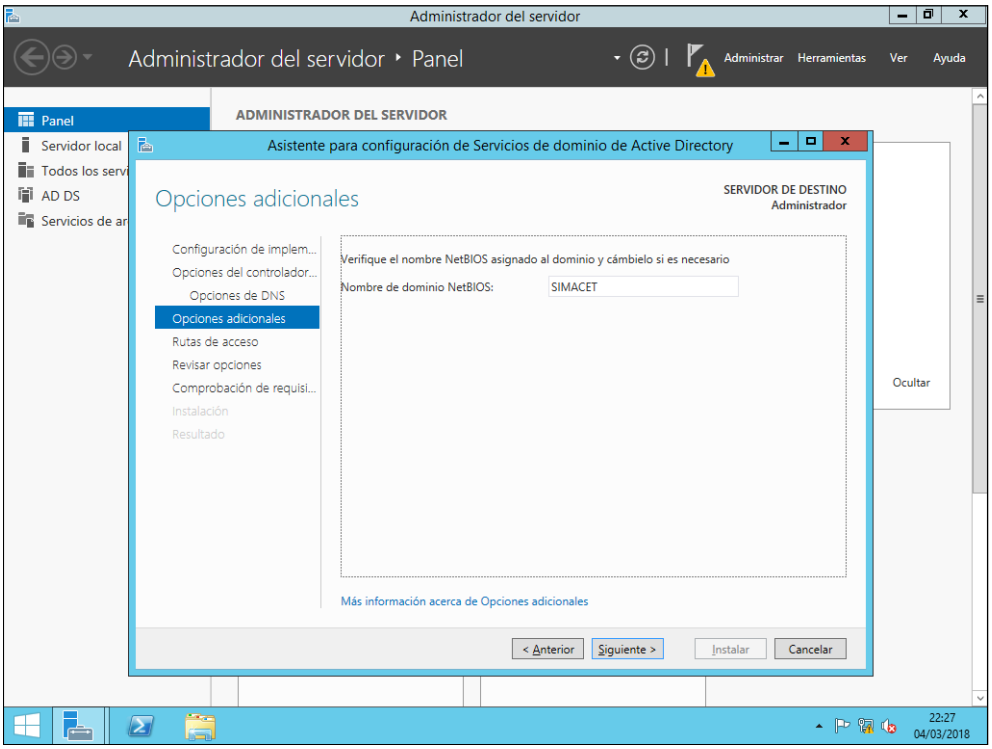


Figura G.21 Configuración dominio NetBIOS
Fuente: elaboración propia

A continuación se hace click sobre “Siguiente”.

Paso 15:

En este paso se seleccionan las rutas de los archivos que Active Directory genera para su almacenamiento y gestión (base de datos, archivos de registro y SYSVOL). Se dejan las que se establecen por defecto:

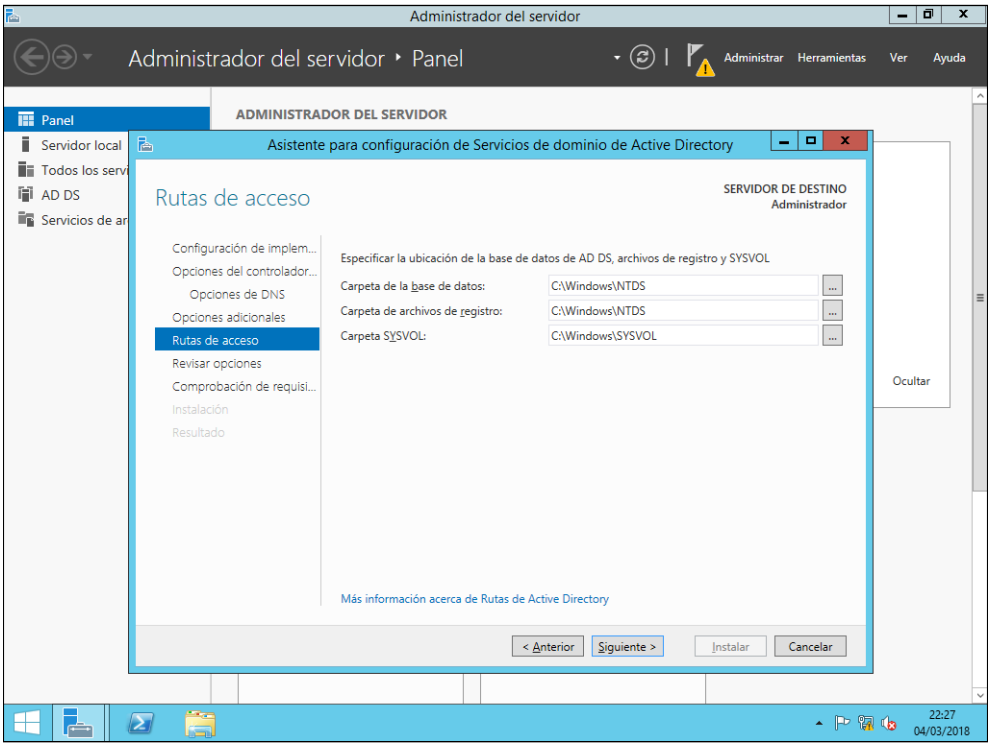


Figura G.22 Selección de rutas de archivos
Fuente: elaboración propia

A continuación se hace click sobre “Siguiente”.

Paso 16:

En este paso se muestran las configuraciones que se han dado en este asistente, para su revisión y posible corrección de errores cometidos:

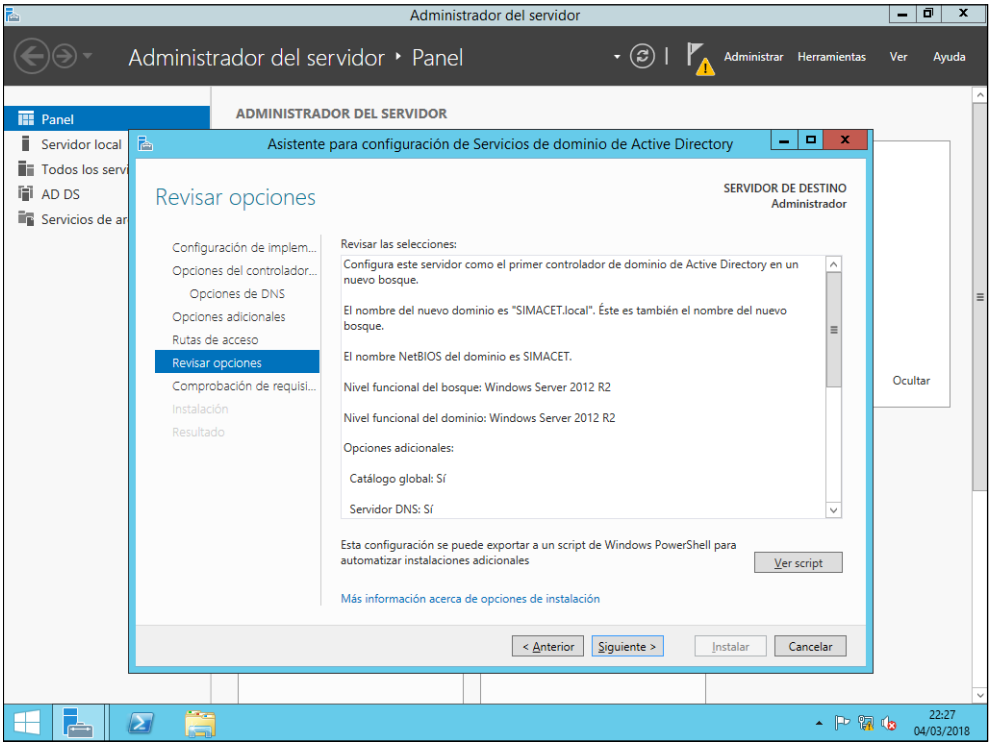


Figura G.23 Comprobación de configuraciones realizadas
Fuente: elaboración propia

Tras haber comprado todos los pasos se hace click sobre “Siguiente”.

Paso 17:

En este paso el asistente hace una comprobación de la configuración establecida en los pasos anteriores. Si esta es correcta, el asistente indica que la comprobación de requisitos se ha realizado correctamente:

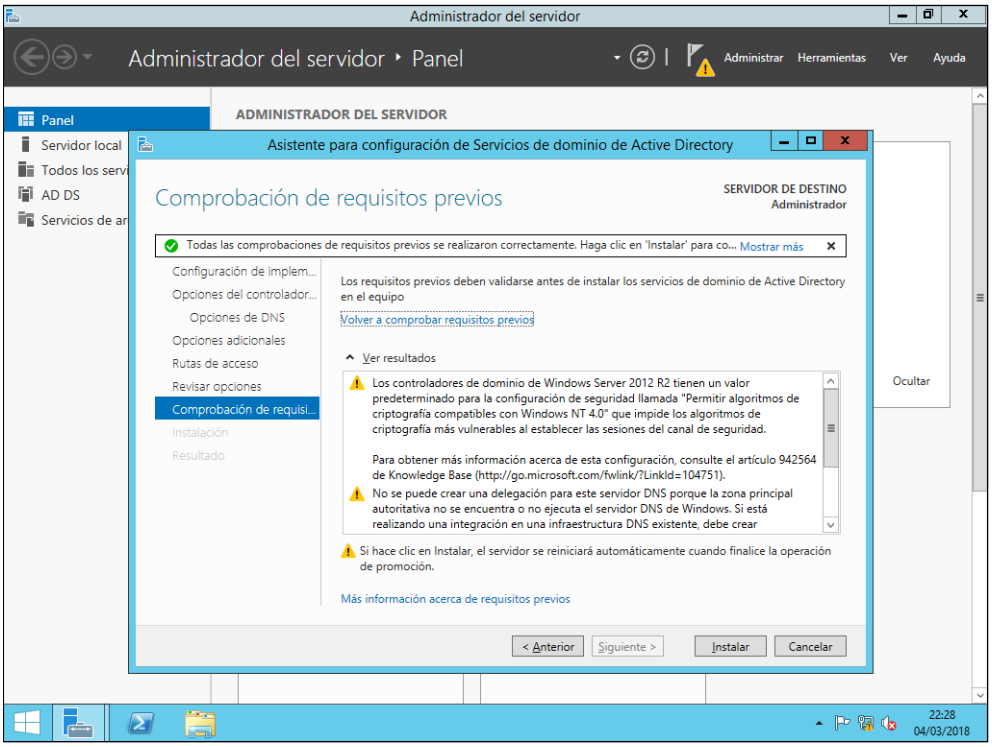


Figura G.24 Comprobación realizada por el asistente
Fuente: elaboración propia

Para continuar y dar inicio a la instalación se hace click sobre “Instalar”.

Paso 18:

En este paso se inicia la instalación:

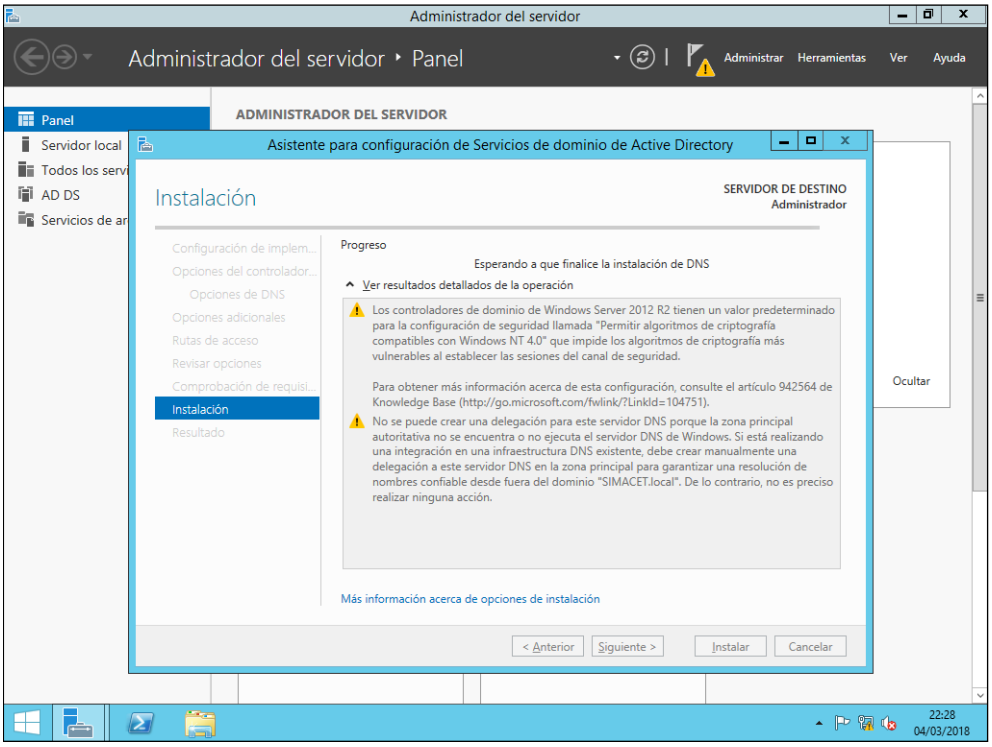


Figura G.25 Inicio de proceso de instalación
Fuente: elaboración propia

Una vez se haya completado la instalación, el asistente reinicia el equipo para establecer las configuraciones realizadas.

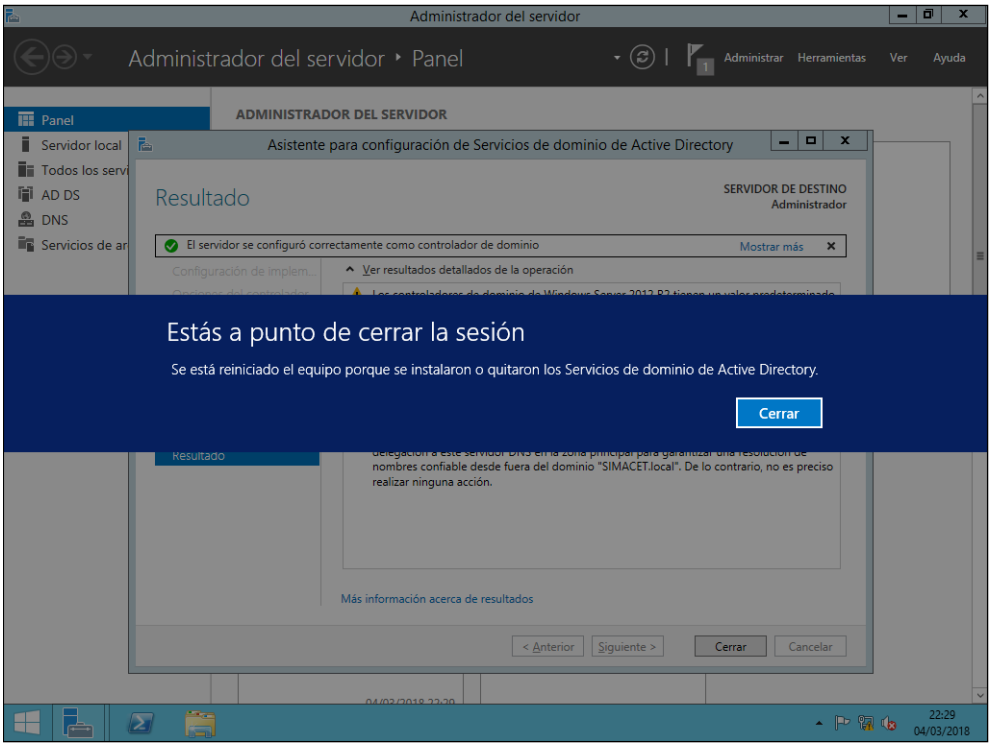


Figura G.26 Reinicio de equipo
Fuente: elaboración propia

Paso 19:

En este paso se comprueba que el dominio ya ha sido creado, puesto que aparece "SIMACET\Administrator". Para acceder al equipo se introduce la contraseña establecida:

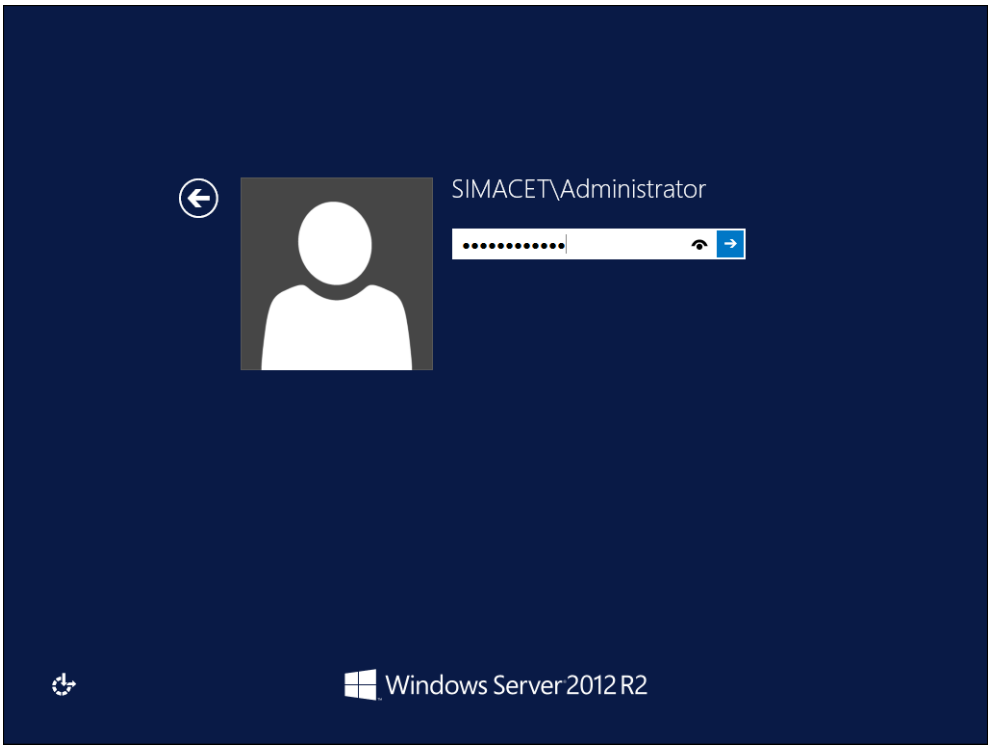


Figura G.27 Acceso al nuevo dominio creado
Fuente: elaboración propia

Paso 20:

En este paso se comprueba que se han instalado correctamente las herramientas del controlador de dominio.

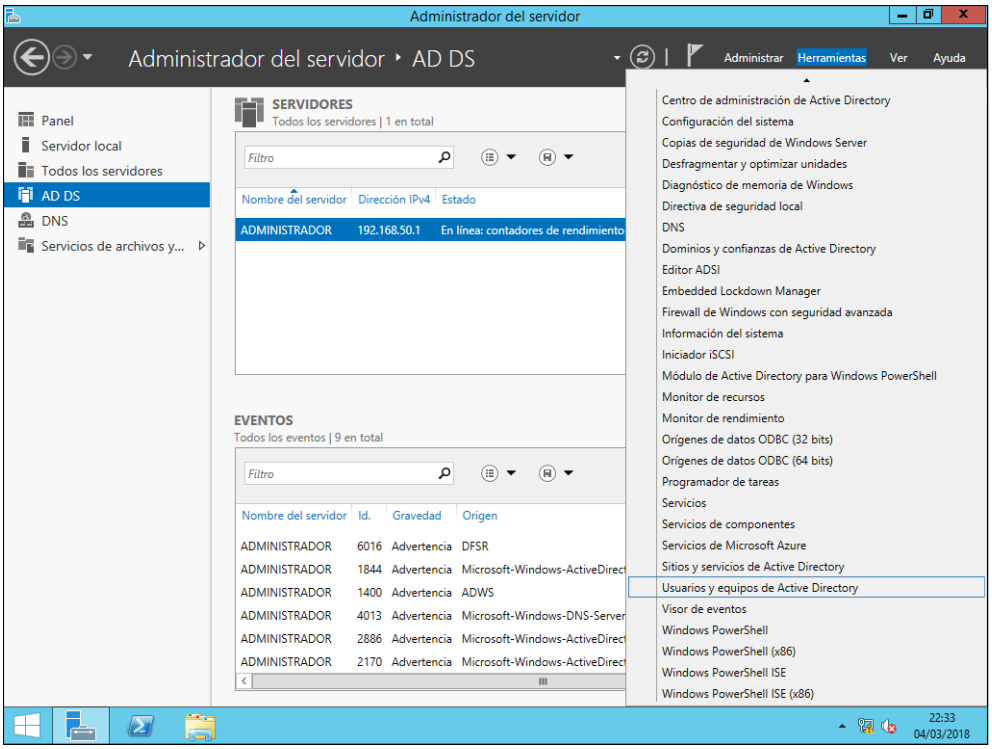


Figura G.28 Comprobación de instalación de herramientas AD DS
Fuente: elaboración propia

Por ejemplo, se comprueba la herramienta “Usuarios y equipos de Active Directory”.

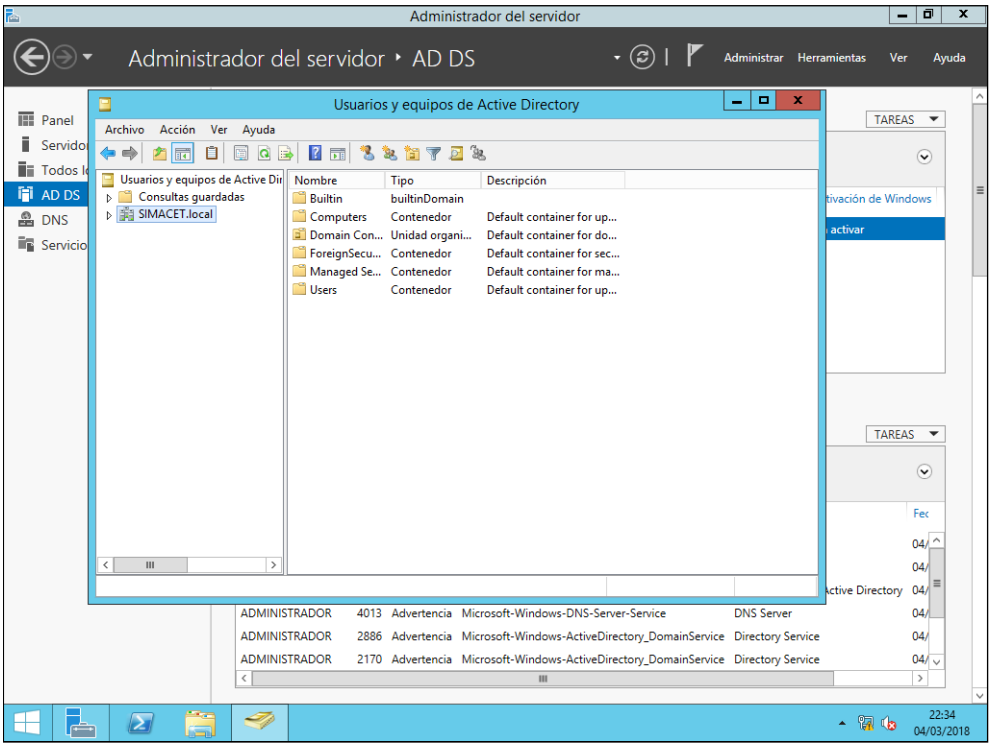


Figura G.29 Comprobación de “Usuarios y equipos de AD DS”
Fuente: elaboración propia

Anexo H: Criterios en valoración de activos esenciales

La valoración de activos conforme a la dimensión disponibilidad se ha realizado siguiendo los siguientes criterios:

- Activo SERV_001:

[7.da] Probablemente cause una interrupción seria de las actividades propia de la Organización con un impacto significativo en otras organizaciones.

- Activo SERV_002:

[5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones.

- Activo SERV_003:

[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.

- Activo SERV_004:

[9.da] Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones.

- Activo INF_001:

[7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.

[7.lbl] Confidencial.

- Activo INF_002:

[6.pi2] Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.

[7.si] Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.

[7.lbl] Confidencial.

- Activo INF_003:

[9.si] Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.

[7.lbl] Confidencial.

Anexo I: Valoraciones acumuladas de activos

Tal y como se ha mencionado, se muestran en este anexo las valoraciones acumuladas de activos, para su correcta visualización:

Tabla I.1 Valoraciones acumuladas de activos
Fuente: elaboración propia

Anexo J: Valoraciones acumuladas de amenazas

Como paso intermedio en el análisis de riesgos, se obtienen las valoraciones acumuladas de las amenazas de cada activo, las cuales se muestran a continuación:

1. Valoraciones acumuladas de amenazas para el activo APP_001:

[APP_001] VMware Workstation			100%		100%
[I.5] Avería de origen físico o lógico		1	50%		
[E.8] Difusión de software dañino		1	10%		10%
[E.20] Vulnerabilidades de los programas (software)		1	1%		20%
[E.21] Errores de mantenimiento / actualización de programas (softwa		10	1%		
[A.8] Difusión de software dañino		1	100%		100%
[A.22] Manipulación de programas		1	50%		100%

Tabla J.1 Valoración de amenazas de activo APP_001
Fuente: elaboración propia

2. Valoraciones acumuladas de amenazas para el activo APP_002:

[APP_002] Sistema Operativo			100%		100%
[I.5] Avería de origen físico o lógico		1	50%		
[E.8] Difusión de software dañino		1	10%		10%
[E.20] Vulnerabilidades de los programas (software)		1	1%		20%
[E.21] Errores de mantenimiento / actualización de programas (softwa		10	1%		
[A.8] Difusión de software dañino		1	100%		100%
[A.22] Manipulación de programas		1	50%		100%

Tabla J.2 Valoración de amenazas de activo APP_002
Fuente: elaboración propia

3. Valoraciones acumuladas de amenazas para el activo APP_003:

[APP_003] Máquina virtual Exchange			100%		100%
[I.5] Avería de origen físico o lógico		1	50%		
[E.8] Difusión de software dañino		1	10%		10%
[E.20] Vulnerabilidades de los programas (software)		1	1%		20%
[E.21] Errores de mantenimiento / actualización de programas (softwa		10	1%		
[A.8] Difusión de software dañino		1	100%		100%
[A.22] Manipulación de programas		1	50%		100%

Tabla J.3 Valoración de amenazas de activo APP_003
Fuente: elaboración propia

4. Valoraciones acumuladas de amenazas para el activo APP_004:

[APP_004] Máquina virtual Sharepoint			100%		100%
[I.5] Avería de origen físico o lógico		1	50%		
[E.8] Difusión de software dañino		1	10%		10%
[E.20] Vulnerabilidades de los programas (software)		1	1%		20%
[E.21] Errores de mantenimiento / actualización de programas (softwa		10	1%		
[A.8] Difusión de software dañino		1	100%		100%
[A.22] Manipulación de programas		1	50%		100%

Tabla J.4 Valoración de amenazas de activo APP_004
Fuente: elaboración propia

5. Valoraciones acumuladas de amenazas para el activo APP_005:

[APP_005] Máquina virtual SIMACET			100%		100%
[I.5] Avería de origen físico o lógico		1	50%		
[E.8] Difusión de software dañino		1	10%		10%
[E.20] Vulnerabilidades de los programas (software)		1	1%		20%
[E.21] Errores de mantenimiento / actualización de programas (softwa		10	1%		
[A.8] Difusión de software dañino		1	100%		100%
[A.22] Manipulación de programas		1	50%		100%

Tabla J.5 Valoración de amenazas de activo APP_005
Fuente: elaboración propia

6. Valoraciones acumuladas de amenazas para el activo APP_006:

[APP_006] Máquina virtual de controlador de dominio			100%		100%
[I.5] Avería de origen físico o lógico		1	50%		
[E.8] Difusión de software dañino		1	10%		10%
[E.20] Vulnerabilidades de los programas (software)		1	1%		20%
[E.21] Errores de mantenimiento / actualización de programas (softwa		10	1%		
[A.8] Difusión de software dañino		1	100%		100%
[A.22] Manipulación de programas		1	50%		100%

Tabla J.6 Valoración de amenazas de activo APP_006
Fuente: elaboración propia

7. Valoraciones acumuladas de amenazas para el activo HW_001:

[HW_001] Servidor físico			100%		100%
[N.1] Fuego		0,1	100%		
[N.2] Daños por agua		0,1	50%		
[N.*] Desastres naturales		0,1	100%		
[I.1] Fuego		0,5	100%		
[I.2] Daños por agua		0,5	50%		
[I.*] Desastres industriales		0,5	100%		
[I.3] Contaminación medioambiental		0,1	50%		
[I.4] Contaminación electromagnética		1	10%		
[I.5] Avería de origen físico o lógico		1	50%		
[I.6] Corte del suministro eléctrico		1	100%		
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%		
[I.11] Emanaciones electromagnéticas		1			1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware		1	10%		
[E.24] Caída del sistema por agotamiento de recursos		10	50%		
[E.25] Pérdida de equipos		0,1	100%		100%
[A.7] Uso no previsto		1	1%		10%
[A.11] Acceso no autorizado		1	10%		50%
[A.23] Manipulación del hardware		0,5	50%		50%
[A.24] Denegación de servicio		2	100%		
[A.25] Robo de equipos		0,1	100%		100%
[A.26] Ataque destructivo		1	100%		

Tabla J.7 Valoración de amenazas de activo HW_001
Fuente: elaboración propia

8. Valoraciones acumuladas de amenazas para el activo HW_002:

[HW_002] Ordenadores de usuario			100%		50%
[N.1] Fuego		0,1	100%		
[N.2] Daños por agua		0,1	50%		
[N.*] Desastres naturales		0,1	100%		
[I.1] Fuego		0,5	100%		
[I.2] Daños por agua		0,5	50%		
[I.*] Desastres industriales		0,5	100%		
[I.3] Contaminación medioambiental		0,1	50%		
[I.4] Contaminación electromagnética		1	10%		
[I.5] Avería de origen físico o lógico		1	50%		
[I.6] Corte del suministro eléctrico		1	100%		
[I.7] Condiciones inadecuadas de temperatura o humedad		1	100%		
[I.11] Emanaciones electromagnéticas		1			1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware		1	10%		
[E.24] Caída del sistema por agotamiento de recursos		10	50%		
[E.25] Pérdida de equipos		5	5%		10%
[A.7] Uso no previsto		1	10%		10%
[A.11] Acceso no autorizado		1	10%		50%
[A.23] Manipulación del hardware		0,5	50%		50%
[A.24] Denegación de servicio		2	100%		
[A.25] Robo de equipos		5	5%		10%
[A.26] Ataque destructivo		1	100%		

Tabla J.8 Valoración de amenazas de activo HW_002
Fuente: elaboración propia

9. Valoraciones acumuladas de amenazas para el activo AUX_001:

[AUX_001] Generador eléctrico			1%
[N.1] Fuego		0,1	1%
[N.2] Daños por agua		0,1	1%
[N.*] Desastres naturales		0,1	1%
[I.1] Fuego		0,5	1%
[I.2] Daños por agua		0,5	1%
[I.*] Desastres industriales		0,5	1%
[I.3] Contaminación medioambiental		0,1	1%
[I.9] Interrupción de otros servicios o suministros esenciales		1	1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware		1	1%
[A.7] Uso no previsto		1	1%
[A.23] Manipulación del hardware		1	1%
[A.25] Robo de equipos		0,5	1%
[A.26] Ataque destructivo		1	1%

Tabla J.9 Valoración de amenazas de activo AUX_001
Fuente: elaboración propia

10. Valoraciones acumuladas de amenazas para el activo AUX_002:

[AUX_002] Sistema de Alimentacion Ininterrumpida			1%
[N.1] Fuego		0,1	1%
[N.2] Daños por agua		0,1	1%
[N.*] Desastres naturales		0,1	1%
[I.1] Fuego		0,5	1%
[I.2] Daños por agua		0,5	1%
[I.*] Desastres industriales		0,5	1%
[I.3] Contaminación medioambiental		0,1	1%
[E.23] Errores de mantenimiento / actualización de equipos (hardware		1	1%
[A.7] Uso no previsto		1	1%
[A.23] Manipulación del hardware		1	1%
[A.25] Robo de equipos		0,5	1%
[A.26] Ataque destructivo		1	1%

Tabla J.10 Valoración de amenazas de activo AUX_002
Fuente: elaboración propia

11. Valoraciones acumuladas de amenazas para el activo AUX_003:

[AUX_003] Refrigeración de equipos			10%
[N.1] Fuego		0,1	10%
[N.2] Daños por agua		0,1	10%
[N.*] Desastres naturales		0,1	10%
[I.1] Fuego		0,5	10%
[I.2] Daños por agua		0,5	10%
[I.*] Desastres industriales		0,5	10%
[I.3] Contaminación medioambiental		0,1	10%
[I.6] Corte del suministro eléctrico		1	10%
[I.9] Interrupción de otros servicios o suministros esenciales		1	10%
[E.23] Errores de mantenimiento / actualización de equipos (hardware		1	10%
[A.7] Uso no previsto		1	10%
[A.23] Manipulación del hardware		1	10%
[A.25] Robo de equipos		0,5	10%
[A.26] Ataque destructivo		1	10%

Tabla J.11 Valoración de amenazas de activo AUX_003
Fuente: elaboración propia

12. Valoraciones acumuladas de amenazas para el activo L_001:

[L_001] Modulares usuarios			100%
[N.1] Fuego		1	100%
[N.2] Daños por agua		1	100%
[N.*] Desastres naturales		0,5	100%
[I.1] Fuego		1	100%
[I.2] Daños por agua		1	100%
[I.*] Desastres industriales		1	100%
[I.3] Contaminación medioambiental		1	10%
[I.4] Contaminación electromagnética		0,1	10%
[A.6] Abuso de privilegios de acceso		1	10%
[A.7] Uso no previsto		1	10%
[A.26] Ataque destructivo		0,1	100%
[A.27] Ocupación enemiga		1	100%

Tabla J.12 Valoración de amenazas de activo L_001
Fuente: elaboración propia

13. Valoraciones acumuladas de amenazas para el activo L_002:

[L_002] Localizacion servidor			100%
[N.1] Fuego		1	100%
[N.2] Daños por agua		1	100%
[N.*] Desastres naturales		0,5	100%
[I.1] Fuego		1	100%
[I.2] Daños por agua		1	100%
[I.*] Desastres industriales		1	100%
[I.3] Contaminación medioambiental		1	10%
[I.4] Contaminación electromagnética		0,1	10%
[A.6] Abuso de privilegios de acceso		1	10%
[A.7] Uso no previsto		1	10%
[A.26] Ataque destructivo		0,1	100%
[A.27] Ocupación enemiga		1	100%

Tabla J.13 Valoración de amenazas de activo L_002
Fuente: elaboración propia

14. Valoraciones acumuladas de amenazas para el activo P_001:

[P_001] Administradores			50%		100%
[E.18] Destrucción de la información		1	1%		
[E.19] Fugas de información		1			10%
[E.28] Indisponibilidad del personal		1	10%		
[A.18] Destrucción de la información		1	10%		
[A.19] Revelación de información		10			50%
[A.28] Indisponibilidad del personal		0,5	20%		
[A.29] Extorsión		0,9	50%		100%
[A.30] Ingeniería social (picaresca)		0,5	50%		100%

Tabla J.14 Valoración de amenazas de activo P_001
Fuente: elaboración propia

15. Valoraciones acumuladas de amenazas para el activo P_002:

[P_002] Usuarios			50%		20%
[E.18] Destrucción de la información		1	1%		
[E.19] Fugas de información		1			10%
[E.28] Indisponibilidad del personal		1	10%		
[A.18] Destrucción de la información		1	10%		
[A.19] Revelación de información		10			20%
[A.28] Indisponibilidad del personal		0,5	50%		
[A.29] Extorsión		0,9	10%		20%
[A.30] Ingeniería social (picaresca)		0,5	10%		20%

Tabla J.15 Valoración de amenazas de activo P_002
Fuente: elaboración propia

Anexo K: Valoraciones de las salvaguardas

Como resultado del análisis de riesgos se obtienen las valoraciones correspondientes a cada salvaguarda, las cuales se muestran a continuación:

1. Valoraciones de la salvaguarda [SW]:

G	PR	[SW] Protección de las Aplicaciones Informáticas (SW)	7
G	AD	[SW.1] Se dispone de un inventario de aplicaciones (SW)	3
G	std	[SW.2] Se dispone de normativa relativa a las aplicaciones (SW)	2
G	proc	[SW.3] Se dispone de procedimientos de uso de las aplicaciones	2
G	EL	[SW.4] IPR: Se protegen los derechos de propiedad intelectual de las aplicaciones (SW)	3
G	EL	[SW.backup] Copias de seguridad (backup) (SW)	5
G	EL	[SW.start] Puesta en producción	3
T	EL	[SW.SC] Se aplican perfiles de seguridad	7
G	EL	[SW.op] Explotación / Producción	5
G	EL	[SW.CM] Cambios (actualizaciones y mantenimiento)	4
G	PR	[SW.end] Desmantelamiento	3

Tabla K.1 Valoración de salvaguardas de [SW]
Fuente: elaboración propia

2. Valoraciones de la salvaguarda [HW]:

G	PR	[HW] Protección de los Equipos Informáticos (HW)	7
G	AD	[HW.1] Se dispone de un inventario de equipos (HW)	2
G	std	[HW.2] Se dispone de normativa sobre el uso correcto de los equipos	2
G	proc	[HW.3] Se dispone de procedimientos de uso del equipamiento	2
G	EL	[HW.start] Puesta en producción	4
T	EL	[HW.SC] Se aplican perfiles de seguridad	7
G	EL	[HW.cont] Aseguramiento de la disponibilidad	6
G	PR	[HW.7] Los medios alternativos están sujetos a las mismas garantías de protección que los habituales	3
G	IM	[HW.8] Contenedores criptográficos (HW, HW virtual)	5
F	EL	[HW.9] {xor} Prevención de emanaciones electromagnéticas (TEMPEST equipment)	5
G	EL	[HW.a] Instalación	3
G	PR	[HW.op] Operación	5
G	EL	[HW.CM] Cambios (actualizaciones y mantenimiento)	4
G	PR	[HW.end] Desmantelamiento	3
G	EL	[HW.PCD] Informática móvil	
G	EL	[HW.f] Maquinas virtuales	
G	EL	[HW.print] Reproducción de documentos	
G	EL	[HW.pabx] Protección de la centralita telefónica (PABX)	
G	EL	[HW.i] Voz, facsímil y video	3

Tabla K.2 Valoración de salvaguardas de [HW]
Fuente: elaboración propia

3. Valoraciones de la salvaguarda [AUX]:

G	PR	[AUX] Elementos Auxiliares	6
G	AD	[AUX.1] Se dispone de un inventario de equipamiento auxiliar	3
T	CR	[AUX.cont] Aseguramiento de la disponibilidad	5
F	EL	[AUX.start] Instalación	4
F	EL	[AUX.power] Suministro eléctrico	4
F	PR	[AUX.AC] Climatización	5
F	EL	[AUX.wires] Protección del cableado	6
G	PR	[AUX.7] Se disponen medidas frente a posibles robos	5
F	IM	[AUX.8] Se prevén medidas frente a todos los problemas graves identificados en el análisis de riesgos	4

Tabla K.3 Valoración de salvaguardas de [AUX]
Fuente: elaboración propia

4. Valoraciones de la salvaguarda [L]:

F	PR	[L] Protección de las Instalaciones	7
F	std	[L.1] Se dispone de normativa de seguridad	2
F	AD	[L.2] Se dispone de un inventario de instalaciones	5
F	EL	[L.3] Entrada en servicio	4
F	EL	[L.design] Diseño	5
T	EL	[L.5] {xor} Existe protección frente a emanaciones (TEMPEST facility zoning)	
F	CR	[L.6] Protección frente a desastres	7
F	RC	[L.cont] Continuidad de operaciones	5
F	PR	[L.end] Desmantelamiento	

Tabla K.4 Valoración de salvaguardas de [L]
Fuente: elaboración propia

5. Valoraciones de la salvaguarda [PS]:

P	PR	[PS] Gestión del Personal	6
P	std	[PS.1] Se dispone de normativa relativa a la gestión de personal (en materia de seguridad)	3
P	proc	[PS.2] Se dispone de procedimientos para la gestión de personal (en materia de seguridad)	3
P	AD	[PS.3] Relación de personal	3
P	PR	[PS.4] Puestos de trabajo	3
P	EL	[PS.5] Contratación	6
P	AD	[PS.6] Cambio de puesto de trabajo	3
P	AW	[PS.AT] Formación y concienciación	3
P	AW	[PS.8] Procedimientos de prevención y reacción	6
P	EL	[PS.9] Protección del usuario frente a coacciones	6
P	EL	[PS.cont] Aseguramiento de la disponibilidad	5
P	AD	[PS.b] Personal subcontratado	

Tabla K.5 Valoración de salvaguardas de [PS]
Fuente: elaboración propia

6. Valoraciones de la salvaguarda [IR]:

G	CR	[IR] Gestión de incidentes	6
G	std	[IR.1] Se dispone de normativa de actuación para la gestión de incidentes	2
G	CR	[IR.2] Se dispone de procedimientos para la gestión de incidentes	5
G	IM	[IR.3] Contención del incidente	6
G	CR	[IR.4] Gestión del incidente	4
G	CR	[IR.5] Cooperación con otras organizaciones	3
G	MN	[IR.6] Comunicación de los incidentes de seguridad	3
G	DC	[IR.7] Comunicación de las deficiencias de seguridad	2
G	MN	[IR.8] Comunicación de los fallos del software	3
G	MN	[IR.9] Se dispone de un registro de incidentes	
G	DC	[IR.a] Los fallos y las medidas correctoras se registran y se revisan	3
G	AD	[IR.b] Control formal del proceso de recuperación ante el incidente	3
P	AW	[IR.c] Formación y concienciación	3
G	AD	[IR.d] Se aprende de los incidentes	3
G	EL	[IR.e] Se toman medidas para prevenir la repetición	4

Tabla K.6 Valoración de salvaguardas de [IR]
Fuente: elaboración propia

7. Valoraciones de la salvaguarda [tools]:

T	PR	[tools] Herramientas de seguridad	8
T	EL	[tools.AV] Herramienta contra código dañino	8
T	DC	[tools.IDS] IDS/IPS: Herramienta de detección / prevención de intrusión	6
T	EL	[tools.conf] Herramienta de chequeo de configuración	
T	MN	[tools.traffic] Herramienta de monitorización de tráfico	
T	MN	[tools.DLP] DLP: Herramienta de monitorización de contenidos	5
T	MN	[tools.HP] Honey net / honey pot	
T	DC	[tools.SFV] Verificación de las funciones de seguridad	6

Tabla K.7 Valoración de salvaguardas de [tools]
Fuente: elaboración propia

8. Valoraciones de la salvaguarda [V]:

G	CR	[V] Gestión de vulnerabilidades	6
G	AD	[V.1] Se dispone de personas dedicadas a la gestión de vulnerabilidades	3
G	AD	[V.2] Se han previsto mecanismos para estar informados de vulnerabilidades ...	4
T	EL	[tools.V] Herramienta de análisis de vulnerabilidades	6
G	AD	[V.4] Se analiza el impacto potencial (estimación de riesgos)	3
G	CR	[V.5] Pruebas de penetración	4
G	proc	[V.6] Se dispone de procedimientos de reacción	3
G	CR	[V.7] Reparación de las vulnerabilidades detectadas	5

Tabla K.8 Valoración de salvaguardas de [V]
Fuente: elaboración propia

9. Valoraciones de la salvaguarda [A]:

T	MN	[A] Registro y auditoría	5
T	AD	[A.1] Administración	4
T	MN	[A.2] Herramientas	4
T	MN	[A.3] Información	5
T	MN	[A.4] Actividades	4

Tabla K.9 Valoración de salvaguardas de [A]
Fuente: elaboración propia

10. Valoraciones de la salvaguarda [BC]:

G	RC	[BC] Continuidad del negocio	5
G	RC	[BC.1] Gestión de la continuidad	3
G	AD	[BC.BIA] Se ha realizado un análisis de impacto (BIA)	2
G	RC	[BC.3] Actividades preparatorias	3
G	RC	[BC.4] Reacción (gestión de crisis)	3
G	RC	[BC.DRP] Plan de Recuperación de Desastres (DRP)	5
T	AD	[BC.6] Restitución (retorno a condiciones normales de trabajo)	2

Tabla K.10 Valoración de salvaguardas de [BC]
Fuente: elaboración propia

11. Valoraciones de la salvaguarda [G]:

G	AD	[G] Organización	4
G	AD	[G.1] Organización interna	3
G	AD	[G.2] Documentación técnica (componentes)	3
G	std	[G.3] Documentación organizativa (normas y procedimientos)	3
G	AD	[G.4] Protección de datos de carácter personal (Documento de seguridad - LOPD)	
G	AD	[RM] Gestión de riesgos	3
G	AD	[G.plan] Planificación de la seguridad	3
G	CR	[G.exam] Inspecciones de seguridad	4
G	EL	[G.8] Salvaguarda de los registros de la Organización (vital records)	

Tabla K.11 Valoración de salvaguardas de [G]
Fuente: elaboración propia

12. Valoraciones de la salvaguarda [E]:

G	AD	[E] Relaciones Externas	5
G	AD	[E.1] Acuerdos para intercambio de información y software	5
G	EL	[E.2] Acceso externo	5

Tabla K.12 Valoración de salvaguardas de [E]
Fuente: elaboración propia

13. Valoraciones de la salvaguarda [NEW]:

G	AD	[NEW] Adquisición / desarrollo					5
G	AD	[NEW.1] Gestión de proyectos					2
G	AD	[NEW.S] Servicios: Adquisición o desarrollo					
G	AD	[NEW.SW] Aplicaciones: Adquisición o desarrollo					5
G	EL	[NEW.HW] Equipos: Adquisición o desarrollo					4
T	AD	[NEW.COM] Comunicaciones: Adquisición o contratación					
G	EL	[NEW.MP] Soportes de Información: Adquisición					
G	cert	[NEW.C] Productos certificados o acreditados					4

Tabla K.13 Valoración de salvaguardas de [NEW]
Fuente: elaboración propia